

DISSERTATION

Sicherheit elektronischer Wahlen -
Eine Methode zur Bewertung und Optimierung der Sicherheit von E-Voting-Systemen

ausgeführt zum Zwecke der Erlangung des akademischen Grades
eines Doktors der technischen Wissenschaften

unter Leitung von
Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Peter Purgathofer
Institut für Gestaltungs- und Wirkungsforschung

eingereicht an der
Technischen Universität Wien
Fakultät für Informatik

von

Mag.rer.soc.oec. Dipl.-Ing. Barbara Ondrisek
Matr.-Nr. 9825622
Mariahilfer Str. 45/64B, 1060 Wien

Wien, Mai 2008 ....

Vorwort

E-Voting ist ein spannendes und politisch brisantes Thema, auch in Österreich, weshalb E-Voting als Thema schnell feststand. Der schwierigere Teil war es, einen wissenschaftlichen, technischen Ansatz zu finden, der auch meine persönliche, kritische Meinung zu elektronischen Wahlen widerspiegelt. Nach langwieriger Recherche und einigen wieder fallen gelassenen Ansätzen entwickelte sich eine solide, qualitative Bewertungsmethode für E-Voting-Systeme (siehe Kapitel 7).

Meinen Dank für Unterstützung bei der Erstellung dieser Arbeit möchte ich an folgende Personen richten: Peter Purgathofer für seinen Enthusiasmus, Gerald Futschek für sein Feedback, Hermann Kaindl für den richtigen Anstoß, Edgar Weippl für den Austausch von Ideen, meinen Lektoren für das geduldige Korrekturlesen und allen Freunden und Bekannten für zahlreiche Diskussionen und Anregungen. Vor allem aber möchte ich Mica für ihre immerwährende und aufopfernde Unterstützung danken.

Anmerkungen zum Format der Arbeit

Anmerkung zur Sprachwahl: Obwohl mehr als die Hälfte aller Personen weltweit weiblich sind[1], wird, für eine leichtere Lesbarkeit, auf das Binnen-I (z. B. „WählerIn“) und die doppelte Schreibweise (z. B. „Wähler und Wählerin“) verzichtet und immer die männliche Form verwendet - was nicht diskriminierend gemeint ist. Von Wortkonstrukten (wie z. B. „Kandidierendenliste“ oder „frau“ statt „man“) wird ebenfalls abgesehen und nur die männliche Stammform der Wörter gebraucht.

Anmerkung zur Verwendung von Internetreferenzen (URL): Alle Webseiten wurden unmittelbar vor der Veröffentlichung dieses Werks auf Gültigkeit überprüft.

[1] 51,58 % der Österreicher sind weiblich. Quelle: Statistik Austria, „Bevölkerung nach Alter und Geschlecht seit 1869 (Österreich)“, für das Jahr 2001.



Zusammenfassung

Sicherheit von E-Voting-Systemen betrifft nicht nur das verwendete Wahlprotokoll oder die eingesetzte Software, sondern das gesamte System inklusive aller Komponenten. Um Sicherheit bei elektronisch gestützten Wahlen zu gewährleisten, muss ein ganzheitlicher Ansatz gewählt werden, der alle Teile dieses komplexen Systems berücksichtigt. Wird nicht jedes Element des Systems auf dessen spezifische Sicherheitsmerkmale, auf Sicherheitsmerkmale der Schnittstellen zu anderen Komponenten und auf dessen Einfluss auf das gesamte System hin überprüft, kann die Sicherheit des gesamten Systems nicht gewährleistet werden.

Um diese These zu untermauern, wurde die *E-Voting-System Security Optimization* Methode (EVSSO-Methode) entwickelt, die zur Bewertung und Optimierung der Sicherheit von E-Voting-Systemen dient. Mit dieser Methode können verschiedene E-Voting-Verfahren bewertet und miteinander vergleichen werden. Die Methode unterscheidet sich von anderen Ansätzen, indem ein ganzheitlicher Ansatz gewählt wird, und die gegenseitigen Abhängigkeiten der verschiedenen Teile eines E-Voting-Systems berücksichtigt werden. Die Sicherheitssituation eines E-Voting-Systems wird zudem anschaulich visualisiert, und dessen Verbesserungspotenzial wird aufgezeigt.

Abstract

Security of e-voting systems does not only concern the voting protocol or the software used, it concerns the whole system including all components. To guarantee security in electronically supported elections a holistic approach which considers all parts of such complex systems has to be chosen. The security of the election system cannot be ensured unless every single element and its security related characteristics, the interfaces to other elements and their impacts on the whole system are examined.

The *E-Voting-System Security Optimization* method (EVSSO-method) is based on this approach and was developed to evaluate and measure the security of e-voting systems. This method also points out security flaws of an examined system, shows its security optimization potential and can be used to compare different electronic voting systems. The methodology differs from other approaches insofar as it is a holistic approach and takes the interdependencies of different aspects of the voting system into account. It visualizes the security situation of an e-voting system in a clear way and shows its potential for improvement.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

E-Voting (zu Deutsch „elektronische Wahlen“), bei dem ein Teil des Wahlvorgangs elektronisch abgebildet wird, ist eine der vielen Anwendungsmöglichkeiten von E-Government. Grundlegend für politische Wahlen ist das Wahlrecht (siehe Kapitel 2), das ebenfalls bei derartigen Wahlverfahren zur Anwendung kommt, und dort gleichermaßen eingehalten werden muss. E-Voting-Systeme (siehe Kapitel 4) sind Computersysteme, deren Zuverlässigkeit - und somit auch das Vertrauen der Wähler in diese - stark von der Sicherheit (siehe Kapitel 3) abhängig ist.

Elektronische Wahlen sind ein umstrittenes Thema, da bereits eine Reihe von (teilweise gravierenden) Sicherheitsmängeln beim Einsatz dieser in der Vergangenheit aufgetreten sind (siehe Kapitel 5). Gegenmaßnahmen zu vielen dieser Risiken (siehe Kapitel 6) wurden bereits von Experten vorgeschlagen, ein neuer Ansatz wird in Kapitel 7 vorgestellt.

In diesem Kapitel wird eine kurze Skizze der These dieser Arbeit, eine allgemeine Einführung in E-Government, ein Überblick über E-Voting, dessen unterschiedliche Ausprägungen sowie Vor- und Nachteile verschiedener Arten von Wahlen gegeben.

1.1 These

Sicherheit von E-Voting-Systemen betrifft nicht nur - wie meist angenommen [Grit03, SaPo06] - das verwendete Wahlprotokoll[2] oder die eingesetzte Software, sondern das gesamte System inklusive aller Komponenten. Um Sicherheit bei elektronisch gestützten Wahlen zu gewährleisten, muss man einen ganzheitlichen Ansatz wählen, der alle Teile dieses komplexen Systems berücksichtigt. Wird nicht jedes Element des Systems auf dessen spezifische Sicherheitsmerkmale, auf Sicherheitsmerkmale der Schnittstellen zu anderen Komponenten und auf dessen Einfluss auf das gesamte System hin überprüft, kann die Sicherheit des gesamten Systems nicht gewährleistet werden.

Um diese These zu überprüfen, wird eine Methode (siehe Kapitel 7) entwickelt, die zur Bewertung und Optimierung der Sicherheit von E-Voting-Systemen dient. Mit dieser Methode können verschiedene E-Voting-Systeme bewertet und miteinander vergleichen werden, Verbesserungspotenziale der Sicherheit eines E-Voting-Systems werden aufgezeigt.

[2] Die Definition des Wahlprotokolls (auch Wahlschema oder -algorithmus genannt) betrifft zum einen die generelle Architektur (z. B. Trennung von Wahl- und Urnenserver), zum anderen die Schritte des Ablaufs der Stimmabgabe (z. B. erster Schritt: Authentifizierung).

1.2 Definition E-Government

Elektronische Interaktionen mit staatlichen Institutionen und Instanzen ergänzen die üblichen Aktionen und Transaktionen der Staatsbürger zunehmend. Es gibt eine Reihe von Definitionen des Begriffs *Electronic Government* oder *E-Government*. Folgende zwei Definitionen gelten als die meistzitierten.

Definition nach Schedler:

„Electronic Government ist eine Organisationsform des Staates, welche die Interaktionen und Wechselbeziehungen zwischen dem Staat und den Bürgern, privaten Unternehmungen, Kunden und öffentlichen Institutionen durch den Einsatz von modernen Informations- und Kommunikationstechnologien (IKT) integriert.“ [Sche01, S. 35]

Die Definition nach Aichhorn / Schmutzer besagt:

„Mit dem Begriff "Electronic Government" (E-Government) wird entsprechend der gegenwärtigen internationalen Diskussion eine neue Phase des Einsatzes von Informations- und Kommunikationstechnologien im Bereich Regierung und öffentliche Verwaltung bezeichnet. Ein wesentlicher Zug ist der verstärkte Einsatz elektronischer Medien im Verkehr zwischen Bürgern und Einrichtungen des politischen Systems (öffentliche Verwaltung, Regierung, Parlament, etc.).“ [AiSc99, S. 7]

Es werden eine Reihe verschiedener Gebiete bei E-Government unterschieden. Die größten Teilbereiche sind Folgende[3]:

- E-Decision: Entscheidungsunterstützung
- E-Democracy und E-Voting: politische Partizipation
- E-Assistance: Unterstützung im Alltag
- E-Administration: Verwaltungsaufgaben
- E-Procurement und E-Fulfillment: Geschäftsabwicklung
- E-Recht: Gesetzeserzeugung und -kundmachung
- E-Payment und E-Card: z. B. Authentifizierung, Bezahlung
- Weitere: z. B. E-Learning

[3] Nach J. Bröthaler: Vortrag „Entscheidungsunterstützung im öffentlichen Sektor - Decision Support in E-Government“. TU Wien, 2007.

E-Voting ist ein entscheidender Teil von E-Government und dient zur demokratischen Entscheidungsfindung.

1.3 Definition E-Voting

E-Voting ist ein eher „fuzzy“, also ein unscharfer Begriff, der oft mit anderen verwandten Begriffen wie Internetwahlen oder Online-Wahlen vermischt wird. Diese kurze Übersicht definiert den Begriff E-Voting und grenzt ihn von ähnlichen Begriffen ab [CESG02, S. 6f].

- Elektronische Wahlen, Electronic Voting oder E-Voting: Damit ist jene Wahlmethode gemeint, bei der die Stimmen der Wähler auf elektronischem Weg repräsentiert oder gesammelt werden.
- Kiosk-Wahlen: Die Verwendung bestimmter Wahlmaschinen in Wahllokalen oder anderen kontrollierten Orten. Die Stimmen werden auf individuellen Maschinen, bekannt als Direct Recording Electronic (DRE) Wahlmaschinen bzw. Wahlcomputer[4], abgegeben und gesammelt. Nach Beendigung des Wahlvorganges werden die abgegebenen Stimmen an eine zentrale Zählstelle (elektronische Urne) weitergeleitet.
- Remote Electronic Voting (REV), elektronische Fernwahlen: Dieser Ausdruck wird für das Wählen über elektronische Mittel von einem entfernten Ort aus verwendet. Das inkludiert das Wählen über das Internet, über Textnachrichten (SMS), interaktives digitales TV oder das Tonwahl Telefon.
- Online-Wahlen: Elektronisches Wählen, während man an ein Live-System angeschlossen ist. Das inkludiert REV wie auch Kiosk-Wahlen, falls bei Letzterem eine ständige Verbindung zu einer zentralen Sammelstelle (Server) gehalten wird.
- Internetwahlen, Internet Voting oder I-Voting: Ein Spezialfall von REV, bei dem (etwa von zu Hause oder von der Arbeit aus) über das Internet wie etwa über eine Website oder ein Applet oder Ähnliches gewählt wird.
- Mobile Wahlen oder M-Voting: Ebenfalls ein Spezialfall von REV, wobei hier die Stimme auf einem Mobiltelefon oder PDA (Personal Digital Assistant) [OnGr05] abgegeben wird.

In anderen Quellen (z. B. [XeMa04]) werden etwas andere Unterscheidungen angegeben, die allerdings weitreichend mit vorheriger übereinstimmen. Der Begriff „E-Voting“ umfasst somit Wahlmaschinen gleichermaßen wie auch Internetwahlen. Eine nähere Betrachtung dieser beiden sehr unterschiedlichen Verfahren wird in Kapitel 1.4 fortgeführt.

[4] Der Begriff „Wahlcomputer“ ist umstritten, wird von Verfechtern von E-Voting Systemen vermieden und gerne durch „Wahlmaschinen“, im Sinne von *Dedicated Special Purpose Machine*, ersetzt (siehe Kapitel 5.4.2.5).

1.3.1 Vorteile und Nachteile von E-Voting

Die Einführung von E-Voting statt oder ergänzend zu Urnenwahlen (siehe auch Kapitel 2.2) ist ein kontroverses Thema. Eine Liste der E-Voting-Initiativen wird im Anhang gegeben (siehe Appendix B).

Vorteile, die von Befürwortern von E-Voting genannt werden, sind schnellere Auszählungen, Modernisierung und Zukunftsorientierung, das Verhindern unabsichtlich ungültiger Stimmen (besonders beim Panaschieren und Kumulieren[5]) und Vorteile für körperlich beeinträchtigte Personen (barrierefreies Wählen). Weiters werden finanzielle Ersparnisse, Steigerung der Wahlbeteiligung, leichtere Einbindung von Wählern aus dem Ausland, ein schnelleres Ergebnis wie auch Anwendung der *direkten Demokratie* genannt [MaPo04].

Der Einsatz elektronischer Wahlen hat, Kritikern zufolge, aber nicht nur Vorteile [BiWa07]. Nachteile sind die mangelhafte Transparenz der Stimmabgabe (siehe auch Kapitel 6.5), fehlende Papierbackups für erneute, aussagekräftige Auszählungen [DiSc03] (siehe auch Kapitel 6.7.1), das für den Bürger oder für die Mitglieder der Wahlkommission nicht verständliche oder nachvollziehbare (transparente) System [ORG07], unaufdeckbare Manipulationsmöglichkeiten des Ergebnisses, schlechte Sicherung der Geräte [CCC06], fehlende Kontrolle für die Wahlkommission (vom Sourcecode bis zum Transfer der Stimme), das blinde Vertrauen in die Soft- und Hardware und nicht zuletzt die Sicherheit des gesamten Systems.

Das Argument der Kosteneinsparung durch den Einsatz von E-Voting konnte durch konkrete Zahlen aus Belgien (parlamentarische Anfragen belegen, dass sich die Kosten pro Wählerstimmer verdreifacht haben), aus England (die Einführung führte zu erheblich höheren Kosten[6]) und durch Studien in Quebec (Steigerung der Kosten um 25 %) [Gyul06] widerlegt werden.

Aus Schweden [Groe02], wie auch aus England, sind auch Entkräftungen des Arguments für die Steigerung der Wahlbeteiligung bei *Multi-Channel Voting*[7] bekannt, da sich die von der Regierung erwartete höhere Wählerbeteiligung bei den Pilotversuchen nicht eingestellt hatte [ORG07]. Eine Steigerung des politischen Interesses scheint somit nicht durch alternative Möglichkeiten der Stimmabgabe, sondern nur durch eine Änderung der demokratischen Kultur möglich zu sein.

---

5 Beim Kumulieren (auch „Häufeln“ genannt) können mehrere Stimmen auf Kandidaten einer Partei abgegeben werden, beim Panaschieren können mehrere verfügbare Stimmen auf Kandidaten unterschiedlicher Listen verteilt werden.

6 Ian Brown vom Oxford Internet Institut und Mitglied der britische Open-Source Rights Group zeigte, dass das Argument der Kosteneinsparungen in England nicht belegt werden konnte, da bei fünf Pilotversuchen bei den Kommunalwahlen Anfang Mai 2007 die Kosten pro Wählerstimme nach offiziellen Angaben umgerechnet zwischen 150 und 900 Euro gelegen haben [Siet07]. Eine Papierstimme kostet im Vergleich dazu etwa 1,5 Euro.

7 Bei Multi-Channel Voting ist die Stimmabgabe via Wahlmaschinen in Wahllokalen, über das Internet oder über Mobiltelefone möglich.

Nach einem Abwägen der Argumente für und wider elektronische Wahlen kann eine Entscheidung über den Einsatz von E-Voting-Systemen getroffen werden. Die Regierung sollte, aus dem Grundsatz der Öffentlichkeit (siehe auch Kapitel 6.5), dabei auch Bürger an der Entscheidungsfindung teilhaben lassen.

1.4 Distanz- und Präsenzwahlen

Im Allgemeinen wird bei E-Voting zwischen Distanz- und Präsenzwahlen unterschieden. Als Unterscheidungskriterium wird hierbei zum einen der Ort der Stimmabgabe, und zum anderen die Anwesenheit einer Wahlkommission zum Zeitpunkt der Stimmabgabe herangezogen [Bran05, S. 714f; KrVo05].

- *Präsenzwahlverfahren*: Jeder Stimmberechtigte kann und soll seine Stimme persönlich unter Aufsicht einer Wahlkommission in einem Wahllokal abgeben. Ein Beispiel für Präsenzwahlen sind gängige Urnenwahlen (siehe auch Kapitel 2.2) oder (elektronisch gestützt) eine Stimmabgabe mit Wahlmaschinen.
- *Distanzwahlverfahren*: Hier entzieht sich der Stimmberechtigte der Aufsicht einer Wahlkommission, in dem er seine Stimme von einem anderen Ort aus abgibt, wie etwa bei Briefwahlen (siehe auch Kapitel 2.3) oder Internetwahlen. Abbildung 1 zeigt die möglichen Datenflüsse einer elektronischen Distanzwahl.

Generell kann gesagt werden, dass die Sicherheit bei Präsenzwahlen leichter zu gewährleisten ist als bei Distanzwahlen, da die Wahlbehörde bei Distanzwahlen im privaten Umfeld die Kontrolle und somit auch die Sicherung verliert. Durch die Aufsicht der Wahlbehörde über die Stimmabgabe kann bei Präsenzwahlen das persönliche und geheime Wahlrecht leichter gesichert werden als bei Distanzwahlen [XeMa04].

1.4.1 Internetwahlen

I-Voting (Wählen über das Internet) - als Spezialfall elektronischer Wahlen (siehe Kapitel 1.3) - ist ein Beispiel für Distanzwahlen und birgt durch die Verknüpfung zum Internet weit höhere Sicherheitsrisiken in sich als andere E-Voting-Verfahren. Den Vorteilen von Internetwahlen, wie Wählen „im eigenen Pyjama", höhere Wahlbeteiligung, Steigerung der Mobilität für Wähler (v. a. Auslandswähler), Kostenersparnisse, breiterer Zugang und weitere Zugriffsmöglichkeiten [MoGl01], werden schwerwiegende Nachteile von Kritikern entgegengehalten.

Zum einen sind diese zusätzlichen Sicherheitsrisiken des I-Votings mit den allgemeinen Sicherheitsproblemen des Internets verbunden, wie der Möglichkeit verschiedener Angriffe wie Hacker Attacken, Phishing, Viren, Trojaner, Lauschangriffe, Malware, Spyware, Rückverfolgbarkeit, etc., vor allem aber *(Distributed) Denial-of-Service* Attacken[8], gegen die es bei jetzigem Stand der Technik keinen hinreichenden Schutz gibt. Das geheime Wahlrecht könnte durch Vorratsdatenspeicherung, Online-Durchsuchungen (etwa mittels Bundestrojaner), Deep Packet Inspection, oder das Ausspionieren von IP Adressen nicht gewährleistet werden, da eine Zuordnung von Stimmen zu Wählern möglich wäre.

[8] (Verteilte) Angriffe auf ein System, bei dem der Zugriff auf jenes verhindert wird, indem das System mit Anfragen überhäuft wird.

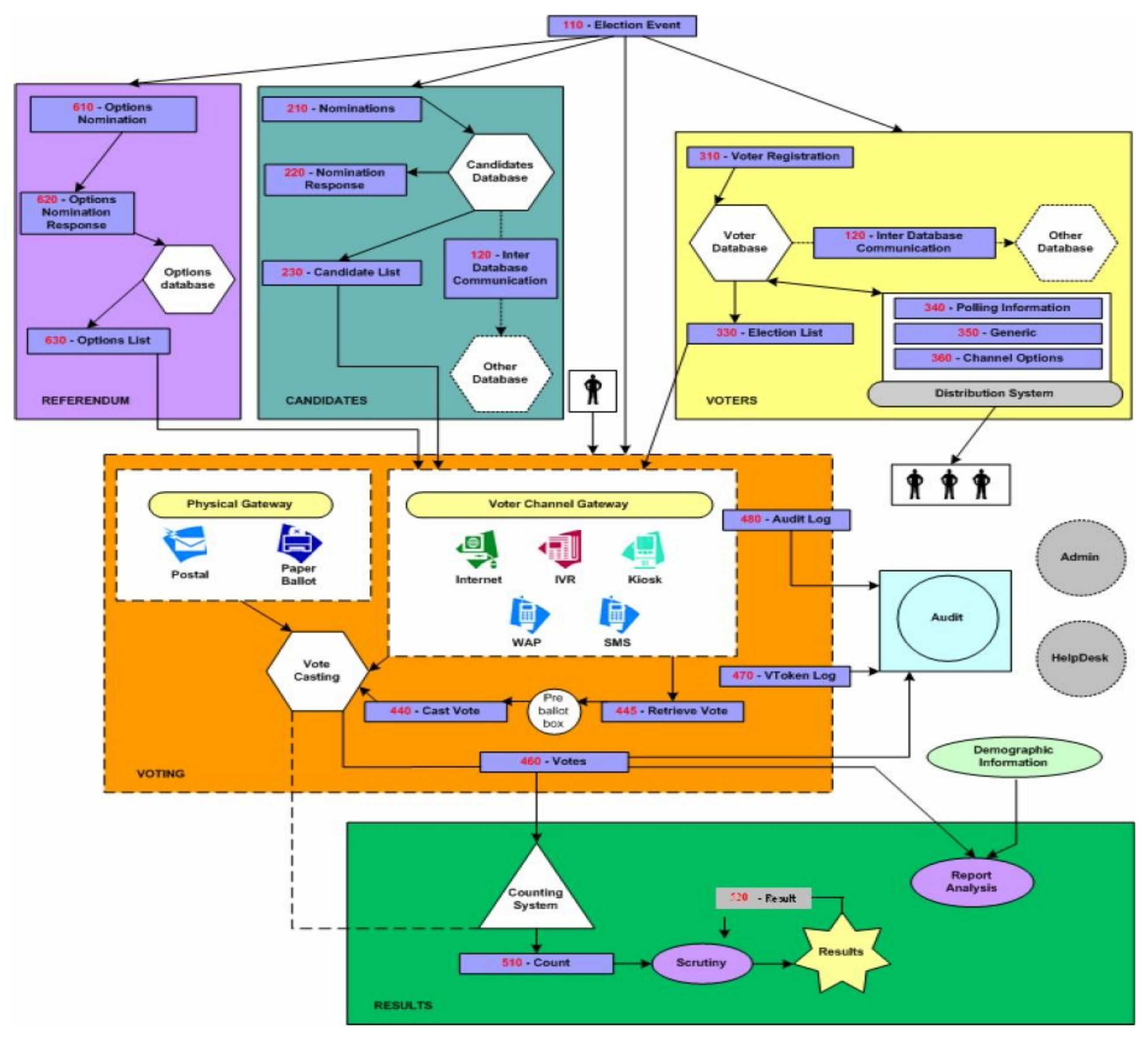


Abbildung 1: Distanzwahlverfahren: End-to-end Lifecycle einer elektronischen Wahl mit Datenflüssen zwischen Prozessen und Datenbanken. Quelle: [OASI07, S. 4]

Zum anderen werden bei Distanzwahlen Methoden der unzulässigen Wählerbeeinflussung erleichtert, wie Erpressung (etwa Anordnungen im Familienkreis, auch *Family Voting* genannt, oder durch andere) und Stimmenkauf, da Wähler beeinflusst werden können, auch ohne dass die Angreifer die Wähler jemals gesehen haben. Zudem befinden sind die Möglichkeiten der Verbrechensverfolgung von Tätern über das Internet - zu deren Gunsten - in einem rechtlichen Graubereich. So sind etwa Angriffe über ausländische Server aus strafrechtlichen Gründen nicht nach österreichischem Recht verfolgbar. Auch stellen Internetwahlen die Gleichberechtigung der Bürger (Bevorzugung von Personen ohne Internet, Technologieverständnis älterer Mitbürger, eventuelle Kosten zusätzlicher Geräte, wie etwa Chipkartenlesegeräten, etc.) vor ein Problem.

Wahlen über das Internet bieten zudem keine Möglichkeit für aussagekräftige Audit-Verfahren[9], wie auch von authentischen, erneuten Auszählungen, da keine Papierbelege verwendet werden können (siehe auch Kapitel 6.7). Die Stimmauszählung erfolgt in einer *Blackbox*[10] und entzieht sich somit vollständig den Augen der Wahlkommission und Wahlbeobachtern, was in Widerspruch zum Öffentlichkeitsprinzip und zum Transparenzgebot steht und den Nachweis von Manipulationsfreiheit unmöglich macht. Damit ist es bei I-Voting-Verfahren äußerst schwierig Transparenz und die Überprüfbarkeit der Richtigkeit des Wahlergebnisses sicherzustellen, wodurch auch das Vertrauen in diese Systeme schwindet. Solche Probleme haften allen Distanzwahlverfahren, wie auch der Briefwahl (siehe Kapitel 2.3), an.

Viele Wissenschaftler, Techniker und Gruppierungen, wie etwa Peter G. Neumann [NeMe00], der Chaos Computer Club in Deutschland oder Ronald L. Rivest vom MIT [BrJe01] und viele andere [DiSi08, JeRu04a, MuVa98, Merc02, Phil02, Rubi02, Wein00] sprechen sich ebenfalls explizit gegen Internetwahlen aus.

> „Remote Internet voting systems pose significant risk to the integrity of the voting process and should not be fielded for use in public elections until substantial technical and social science issues have been addressed. The security risk associated with these systems are both numerous and pervasive and, in many cases, cannot be resolved using even today's most sophisticated technology.“ [IPI01, S. 19]

Aus diesem Grund werden Internetwahlen in dieser Arbeit nicht behandelt und nur der Vollständigkeit halber gestreift (siehe auch Kapitel 4.3.3). Der Fokus liegt eindeutig auf Wahlmaschinen, im Speziellen auf DRE-Wahlcomputer, im Sinne der Definition in Kapitel 1.3.

---

[9] Audits bezeichnen allgemeine Untersuchungsverfahren.

[10] Blackbox (engl. „Schwarze Schachtel“) ist ein Objekt, dessen innere Funktion und der Aufbau unbekannt ist. Das Gegenstück dazu ist die *Whitebox*.

2 Wahlrecht

Das bestehende Wahlrecht einer Demokratie ist die Basis jedes E-Voting-Systems. Im Allgemeinen gilt für jede einzelne Wahl ein etwas anderes Recht. Die (aktiven[11]) Wahlen der Österreichischen Hochschülerschaft sind etwa anders festgelegt als die Nationalratswahlen, aber bei jeder Wahl wird nach ähnlichen Grundsätzen gewählt: Vor dem tatsächlichen Wahlvorgang muss die Identität des Stimmberechtigten verifiziert, die Unverfälschtheit des ausgefüllten Stimmzettels garantiert, die freien Willensentscheidung gesichert und der Übereilungsschutz[12] gewährt werden (siehe auch Kapitel 2.2).

2.1 Wahlgrundsätze

Das Wahlrecht ist in folgenden in Verfassungsrang stehenden Bestimmungen verankert: Bundes-Verfassungsgesetz [BGBl30] Artikel 23a (Europäisches Parlament), Artikel 26 (Nationalrat), Artikel 60 (Bundespräsident), Artikel 95 (Landtag), Artikel 117 (Gemeinderat), Artikel 8 des Staatsvertrages von Wien [BGBl55] (geheimes und allg. Wahlrecht) und Artikel 3 des ersten Zusatzprotokolls zur Konvention der Menschenrechte und Grundfreiheiten (freies Wahlrecht) [Dujm00, Lann04].

Zusammenfassend lässt sich sagen, dass in Österreich aufgrund des allgemeinen, freien, gleichen, unmittelbaren, geheimen und persönlichen Wahlrechts die Möglichkeit besteht, an der Wahl zum Landtag, zum Nationalrat, zum Gemeinderat, zum Europaparlament und des Bundespräsidenten teilzunehmen, wobei sich die Wahlrechte untereinander im Mindestalter der Wahlberechtigten unterscheiden.

Die Wahlgrundsätze im Einzelnen [WaMa00, Rose00]:

- *Allgemeines Wahlrecht* (Art. 26 Abs. 1 und 4 B-VG, Art 8 StV v Wien): Es steht grundsätzlich allen Staatsbürgern, ab einem bestimmten Mindestalter, abhängig vom ordentlichen Wohnsitz[13], ohne Unterschied von Rasse, Geschlecht, Sprache, Religion oder politischer Meinung zu zu wählen. Nicht österreichische EU-Bürger dürfen an Gemeinderatswahlen bzw. in Wien an Bezirksvertretungswahlen, sowie an Europawahlen teilnehmen. Ausnahmen bestehen etwa bei Personen mit gerichtliche Verurteilungen.

[11] Das aktive Wahlrecht, bei dem Wähler ihre Stimme abgeben, steht im Gegensatz zum passiven Wahlrecht, wo ein Kandidat von Wählern gewählt werden kann.

[12] „Übereilungsschutz“ bedeutet, dass man den ausgefüllten Stimmzettel vor der Stimmabgabe nochmals sehen und so seine Stimme überprüfen kann, bevor man den Stimmzettel endgültig abgibt.

[13] Nach dem Erkenntnis des Verfassungsgerichtshofes [VfGH89] wird Auslandsösterreichern ein fiktiver Wohnsitz zugeordnet, damit sie dort wählen können.

- *Freies Wahlrecht* (Art 8 StV v Wien, Art 3 1. ZProtMRK): Dem Wähler wird die Entscheidungsfreiheit gesichert. Weder in die Aufstellung der Wahlvorschläge, noch in die Wahlwerbung oder in die Ausübung des aktiven oder passiven Wahlrechts darf von dritter Seite eingegriffen werden. Es muss die Möglichkeit geben, frei aus mehreren Kandidaten oder Parteien auszuwählen, auch die Kandidatenaufstellung muss frei sein.
- *Gleiches Wahlrecht* (Art 26 Abs 1 B-VG, Art 8 StV v Wien): Jeder Wähler verfügt über die gleiche Zahl von Stimmen und jede Stimme zählt gleich.
- *Unmittelbares Wahlrecht* (Art 26 Abs 1 B-VG): Wähler können die Abgeordneten ohne eine Zwischenstufe, also ohne Wahlmänner (vgl. USA) oder andere mittelbare Instanzen, wählen.
- *Geheimes Wahlrecht* (Art 26 Abs 1 B-VG, Art 8 StV v Wien): Der Wähler trifft seine Wahlentscheidung in einer für die Öffentlichkeit und die Wahlbehörde nicht erkennbaren Weise. Geeignete Einrichtungen (z. B. Wahlzellen, Wahlkuvert, Wahlurne, etc.) müssen zur Verfügung gestellt werden. Somit wird auch die Nachweisbarkeit der Stimme für andere (Stimmenkauf) verhindert und das Wahlgeheimnis gesichert.
- *Persönliches Wahlrecht* (Art 26 Abs 1 B-VG): Der Wahlberechtigte übt seine Stimmabgabe selbst und nicht durch einen Stellvertreter aus. Ausgenommen sind sinnes- oder körperbehinderte Bürger, die das Ausfüllen des Stimmzettels ohne fremde Hilfe nicht vornehmen können.
- *Verhältniswahlrecht* (Art 26 Abs 1 B-VG): Im Gegensatz zum Mehrheitswahlrecht[14] wird allen politischen Kräften von zahlenmäßig erheblicher Bedeutung eine Vertretung im Parlament nach Maßgabe ihrer Stimmenstärke gesichert (außer bei der Direktwahl des Bundespräsidenten).

Ein weiterer Grundsatz gehört zwar nicht unmittelbar zu den „klassischen“ Wahlrechtsgrundsätzen, vervollständigt diese aber:

- *Öffentlicher und transparenter Wahlvorgang* (Art. 1 § 49 EuWO, § 61 Nationalrats-Wahlordnung 1992): Mitglieder einer Wahlkommission, Wahlzeugen [BGBl96 Art. 1 § 49, BGBl92 § 61] und externe (internationale) Wahlbeobachter haben die Möglichkeit, den Wahlvorgang zu verfolgen, „ein weiterer Einfluss auf den Gang der Wahlhandlung steht ihnen nicht zu“ [BGBl96 Art. 1 § 47]. Die Auszählung der Stimmen darf in Österreich von Wahlbeobachtern der OECD oder von Wahlzeugen[15] beobachtet werden.

[14] Das Mehrheitswahlrecht wird auch in Österreich angewendet, allerdings nur für die Direktwahl der Bürgermeister und des Bundespräsidenten.

[15] Quelle: Telefonat mit Mag. Robert Stein, Bundesministerium für Inneres, Sektion III - Recht, Abt. III/6 - Wahlangelegenheiten vom 17.4.2008.

Diese Grundsätze gelten in den meisten westlichen Demokratien, etwa ist das deutsche Wahlrecht in Artikel 38 des Grundgesetzes verankert und dem Österreichischen sehr ähnlich. Ausnahmen bilden z. B. die Präsidentschaftswahlen in den USA, bei denen kein unmittelbares Wahlrecht, sondern Wählen durch Wahlmänner zur Anwendung kommt. Diese Grundsätze werden in verschiedenen Staaten allerdings oft unterschiedlich ausgelegt und hängen vom jeweiligen Kontext ab. So gibt es in Deutschland, neben dem Listenwahlrecht[16], die Möglichkeit den Mandatar direkt ohne Zuordnung zu einer Partei zu wählen (Persönlichkeitswahlrecht). In den USA gilt das Mehrheitswahlrecht.

Für die Einhaltung des Wahlrechts und die Durchführung einer Wahl sind die Wahlbehörden zuständig. Die oberste Wahlbehörde, die Bundeswahlbehörde, wird anlässlich jeder Nationalratswahl neu gebildet. Wahlbehörden (insgesamt mehr als 15.000 sorgen für die Durchführung etwa der Nationalratswahl) gibt es neben der Bundesebene auch noch auf Landes-, Bezirks-, Gemeindeebene und auf der Ebene der Wahlsprengel.

2.2 Urnenwahl

Die derzeitige Wahl mit Papierstimmzettel, auch Urnenwahl, genannt (vgl. Distanzwahl, Kapitel 1.4), wird durch folgende bestimmte Aktionen (nach deutschem Recht[17]) durchgeführt [UlKo01]:

Voraussetzung: Das Wählerverzeichnis sei ordnungsgemäß geführt und abgeschlossen.

1. Die Wahlbenachrichtigung wird dem Wähler offen per Post übermittelt.
2. Der Wahlvorstand initialisiert die Urne.
3. Der Wähler zeigt dem Wahlvorstand seine Wahlberechtigung (optional).
4. Der Wähler erhält vom Wahlvorstand einen Wahlumschlag und einen leeren Stimmzettel.
5. Der Wähler füllt den Stimmzettel aus.
6. Der Wähler legt den ausgefüllten Stimmzettel in den Wahlumschlag.
7. Der Wähler gibt die Wahlbenachrichtigung an den Wahlvorstand.
8. Der Wähler zeigt das das Authentisierungsmerkmal des Wählers dem Wahlvorstand.
9. Der Wahlvorstand vergleicht das Authentisierungsmerkmal des Wählers mit dem Identitätsmerkmal des Wählers.

[16] Bei dem Listenwahlrecht (bzw. Parteienwahlrecht) nach dem D'Hondt Verfahren (oder auch Jefferson- oder Hagenbach-Bischoff-Verfahren genannt) werden die Stimmen proportional auf die Sitze verteilt.

[17] Die Schritte der Stimmabgabe sind nach Deutschem Recht beschrieben, jene für eine Stimmabgabe nach Österreichischem Recht werden die Schritte 7-10 vor Schritt 4 ausgeführt.

10. Der Wahlvorstand überprüft, ob der identifizierte Wähler im Wählerverzeichnis als Wähler eingetragen und ob er noch nicht als „hat schon gewählt“ markiert ist.
11. Der Wahlvorstand überprüft den Wahlumschlag auf Richtigkeit und Verschlossenheit.
12. Der Wahlvorstand gibt die Urne für den identifizierten Wähler frei.
13. Der Wähler wirft seinen Umschlag in die freigegebene Urne.
14. Der Wahlvorstand markiert den identifizierten Wähler als „hat schon gewählt“.
15. Der Wahlvorstand sperrt die Urne.
16. Der Wahlvorstand sperrt die Urne endgültig und gibt sie zur Auszählung frei.

Die Stimmzettel werden in Österreich so lange aufbewahrt, bis die Wahl unanfechtbar feststeht. Dabei gilt eine Frist von vier bis sechs Wochen. Danach werden die Stimmzettel vernichtet.[18] In Deutschland werden die Stimmzettel nach der Auszählung, in versiegelten Paketen gesichert, bis maximal 60 Tage vor der nächsten Wahl bei der Gemeindebehörde aufbewahrt.

Aus den Bestimmungen der Stimmabgabe bei der herkömmlichen Wahl lassen sich Sicherheitsanforderungen und Security-Policies ableiten, die auch bei elektronischen Wahlen einzuhalten sind, etwa Identifikation, Authentisierung, Anonymität, etc. Ein E-Voting-System hat somit auch die Anforderung, mindestens so sicher zu sein und ordnungsgemäß abzulaufen wie das konventionelle Wahlverfahren mit Papierstimmzettel.

2.3 Briefwahl

Die Briefwahl bezeichnet die Möglichkeit, seine Stimme außerhalb des Wahllokals per Post aufzugeben und bildet somit die klassische Art der Distanzwahl. Probleme bei Briefwahlen betreffen vor allem die Möglichkeit der unzulässigen Wählerbeeinflussung, wie Stimmenkauf oder Erpressung, und die Einhaltung des geheimen und persönlichen Wahlrechts, da die Behörden die Aufsicht über die Stimmabgabe verlieren (vgl. Kapitel 1.4). Briefwahlen werden zwar in vielen Ländern (wie z. B. den Vereinigten Staaten und Deutschland) praktiziert, in Österreich (wie auch z. B. in Israel und Brasilien) waren sie aber bis vor kurzem bei Wahlen zu Gebietskörperschaften verboten.

In der Schweiz werden Briefwahlen seit 1994 praktiziert und von Seiten der Bevölkerung sehr gut aufgenommen, wobei über 90 % aller Wähler in Basel-Stadt und Genf ihre Stimmen brieflich abgeben [Brau03]. In Deutschland werden Briefwahlen bereits seit 1956 ohne weit reichende Bedenken, wie in Österreich, eingesetzt. [DBtg02]

In seinem Erkenntnis [VfGH85], dem sogenannten *Briefwahlerkenntnis*, hat der Verfassungsgerichtshof 1985 die Briefwahl anlässlich der Prüfung der niederösterreichischen Wahlordnung für

[18] Quelle: Telefonat mit Mag. Robert Stein, Bundesministerium für Inneres, Sektion III - Recht, Abt. III/6 - Wahlangelegenheiten vom 17.4.2008.

Statutarstädte[19] für verfassungswidrig erklärt. Der Erkenntnis beinhaltet, dass die Briefwahl sowohl gegen den Grundsatz der geheimen Wahl als auch gegen den der persönlichen Wahl verstoße. Der Staat trage nichts zur Sicherung der geheimen Wahl bei, und der Wähler bleibe zur Sicherung des geheimen Wahlrechtes vollkommen auf sich selbst gestellt. Weiters handle es sich bei der Briefwahl nicht um eine persönliche Stimmabgabe, im Sinn des Wortlauts zum Zeitpunkt der Entstehung der Verfassung [Mars00].

Die strikte Haltung des Verfassungsgerichtshofes wurde in der Zwischenzeit durch die Einführung der (Auslands-)Wahlkarten[20] und in weiterer Folge durch die Einführung der Briefwahl 2007 aufgegeben, allerdings ist die Stimmabgabe mittels dieser Methode an zusätzliche Bedingungen gebunden. Die Identität des Stimmberechtigten wird beim Abholen der Wahlkarte etwa durch Überprüfung eines amtlichen Lichtbildausweises verifiziert. Die Identifizierung des Wählers kann je nach Gemeinde unterschiedlich sein. Zusätzlich muss auf dem Umschlag, mit dem die Wahlkarte an die Wahlbehörde zurückgesendet wird, eine eidesstattliche Erklärung unterschrieben werden, dass man den „Stimmzettel persönlich, unbeobachtet und unbeeinflusst ausgefüllt“ [BGBl07] hat.

Die Wahlkarte besteht aus zwei Teilen: einem Stimmzettel mit Umschlag und einem A4-Kuvert (siehe Abbildung 2). Die Rückseite des Kuverts ist mit den Daten des Wählers und die Vorderseite mit der Adresse der jeweils zuständigen Wahlbehörde beschriftet.

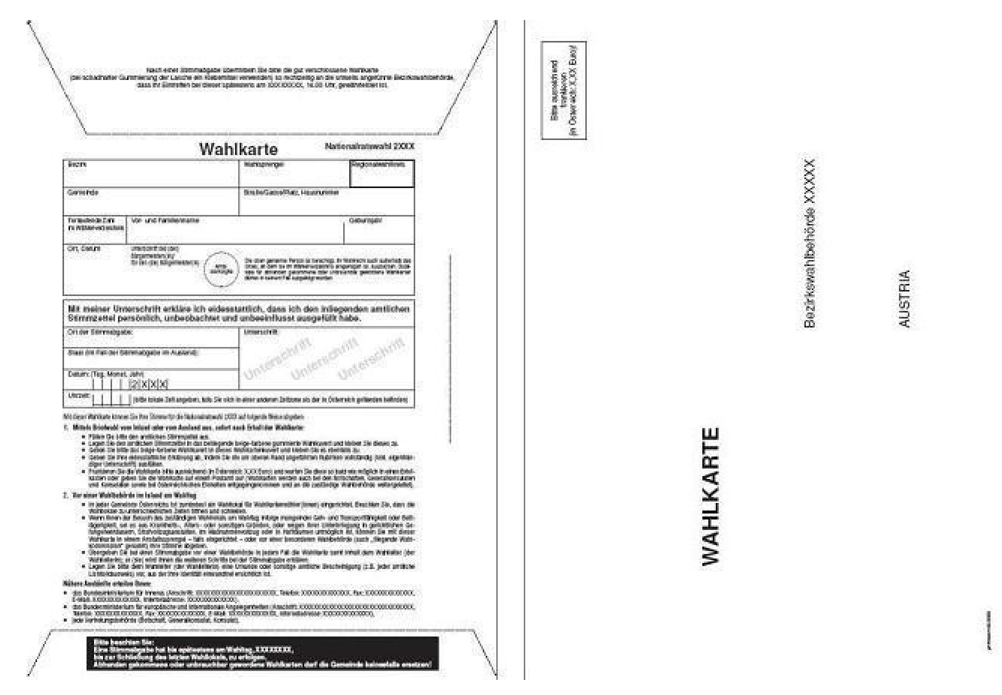


Abbildung 2: Beispiel einer Wahlkarte (von hinten und vorne), Quelle [BGBl07]

[19] Statutarstädte: „Stadt mit eigenem Statut“, d.h. eine Stadt, die im Gegensatz zu übrigen Städten ein eigenes Stadtrecht (Stadtstatut) hat.

[20] Im englischen Sprachraum „Absentee Ballot“ genannt.

Vor der Wahlrechtsänderung durfte die Wahlkarte nur im Ausland abgegeben werden und musste vonseiten einer österreichischen Vertretungsbehörde, eines Notars oder einer ähnlichen Einrichtung, des Einheitskommandanten oder von einem Zeugen mit österreichischer Staatsbürgerschaft auf dem Umschlag gegengezeichnet werden. Mit dem Wahlrechtsänderungsgesetz 2007, das am 1. Juli 2007 in Kraft getreten ist, kann die Wahlkarte in Österreich auch per Post im Inland abgeschickt werden. Weiters kann man mit einer Wahlkarte auch den Wahlsprengel wechseln und kann so zum Beispiel beim Urlaub im dortigen Wahllokal wählen. Der in der Wahlkarte enthaltene Umschlag wird vor der Stimmabgabe im Wahllokal durch einen Umschlag mit der Bezeichnung des Heimatwahlkreises ersetzt. Der Stimmzettel bleibt gleich und wird - wie üblich - persönlich ausgefüllt und im Umschlag in die Urne geworfen wird. Der Staat kann hier die geforderten Vorkehrungen zur Durchführung einer geheimen Wahl garantieren. Die Wahlkarten werden nach Wahlschluss nicht im Wahlsprengel gezählt, wo sie abgegeben wurden, sondern gesammelt und an die jeweils zuständige Wahlbehörde geschickt, um die Stimmen korrekt zuzuordnen.

Die Wahlkarten-Regelung ist allerdings umstritten. Letzten Endes wird hier dem allgemeinen Wahlrecht gegenüber dem persönlichen und dem geheimen Wahlrecht der Vorzug gegeben. Elektronische Wahlen (insbesondere Wahlen über das Internet) gleichen in vielerlei Hinsicht der Briefwahl, da der Wähler auch nicht persönlich in der Wahlzelle seinen Stimmzettel ausfüllt. Nach der Änderung des Wahlrechts hin zur Briefwahl bleibt nun offen, ob es ebenfalls zu einer Änderung in Richtung E-Voting kommen wird, da elektronische Wahlen derzeit nicht zulässig sind und nur durch einen Beschluss des Verfassungsgesetzgebers ermöglicht werden könnten (siehe auch Kapitel 4.5.3).

2.4 Interpretation des Rechts im Bezug auf E-Voting

Die Entscheidung, ob die elektronische Wahl zulässig ist oder nicht, fällt also in den rechtspolitischen Handlungsspielraum des Verfassungsgesetzgebers, wobei auf die technischen Richtlinien und Sicherheitsanforderungen besonderer Wert gelegt werden muss. Eine Reihe von Arbeiten [Hein03, Krim02, Menz02] behandeln die Interpretation des Rechts im Hinblick auf E-Voting. Zusammenfassend kann gesagt werden, dass elektronische Wahlen über das Internet (oder mit mobilen Geräten) der Briefwahl bzw. der Wahl mit Wahlkarten ähneln, wobei es hier zu einem Abwägen zwischen dem allgemeinen Wahlrecht auf der einen Seite und dem persönlichen und geheimen Wahlrecht auf der anderen Seite kommt (siehe Kapitel 1.4). Im Fall der Wahlkarten und der Einführung der Briefwahl in Österreich wurde gezeigt, dass dem allgemeinen Wahlrecht der Vorzug zu geben ist, was somit auch zu einem Argument für E-Voting wurde. Die heutige rechtliche Situation in Österreich schließt aber elektronische Wahlen weiterhin aus (siehe auch Kapitel 4.5).

3 Sicherheit

Neben den rechtlichen Grundlagen ist die Sicherheit bei Wahlvorgängen für E-Voting-Systeme äußerst wichtig. Es können viele verschiedene Aspekte von Sicherheit unterschieden werden (siehe auch Kapitel 3.1.3), jeder davon ist für das Vertrauen in das System unerlässlich. Ein gültiges Wahlergebnis kann nur erzielt werden, wenn alle Komponenten des Wahlsystems sicher entworfen, entwickelt, eingesetzt, gewartet und regelmäßig im Einsatz auf Sicherheit überprüft werden. Wird der Sicherheitsaspekt bei lediglich einer Komponente des Systems kompromittiert oder ausgelassen, so ist das System weiterhin angreifbar.

In diesem Kapitel wird ein Überblick über Sicherheit, Risiken, Einschätzungsmethodiken und allgemeine Abwehrmaßnahmen gegeben, die auch für elektronische Wahlsysteme relevant sind.

3.1 Unterscheidung von Security und Safety

Im angelsächsischen Raum gibt es eine Unterscheidung zwischen den Worten *Security* und *Safety*, die im deutschsprachigen Raum beide gleich bedeutend mit dem Wort *Sicherheit* sind. Beide Begriffe beschäftigen sich mit Bedrohungen oder Risiken und dem Schutz vor oder dem Umgang mit dem Auftreten von Fehlern, die die Verletzung eines Wertes, wie Gefährdung von Menschenleben oder intellektuellem Eigentum, bedeuten.

In der Fachliteratur gibt es eine Vielzahl von Interpretationen der Unterscheidung dieser beiden Aspekte von Sicherheit. Das heute meist verbreitete Verständnis von Safety und Security in Zusammenhang mit Softwaresystemen wird von Andrew S. Tanenbaum beschrieben:

> „Safety refers to the situation that when a system temporarily fails to operate correctly, nothing catastrophic happens." [TaSt02, S. 363]

Safety betrifft somit Schutz vor unachtsamen oder versehentlichen Fehlern und Unfällen. Das Versagen von Safety führt zu Verlusten, Katastrophen oder anderen schwer wiegenden Folgen [Lapr92, S. 4; Leve83].

> „Security is a condition of safety from threads and any threatening event can lead to worry. [..] Security is achieved by a set of safeguards and countermeasures applied to maintain the condition of being safe from threads." [Schu03]

Security, im Gegensatz zu Safety, gilt als der Schutz vor absichtlichen, bösartigen Angriffen und unautorisierten Zugriffen [Lapr92, S. 4; Leve86, S. 137; Leve95, S. 183].

Weitere Interpretationen der Begriffe Safety und Security sind die Folgenden: Ein System, das als *safe* bezeichnet wird, bietet Schutz vor Fehlern vertrauenswürdiger Benutzer, wie zum Beispiel Eingabefehlern. Ein System, das als *secure* bezeichnet wird, kann sich gegen beabsichtigte, bösartige Fehler bzw. Fehler, die von nicht vertrauenswürdigen Benutzern durchgeführt werden, schützen, wie zum Beispiel Angriffe, die zu einem Ausfall des Systems führen [AlAr98]. Eine andere Definition unterscheidet Safety und Security als Schutz vor unbeabsichtigtem im Gegensatz zu absichtlich verursachtem (bösartigem) Schaden [Fire03].

3.1.1 Zusammenhang von Security und Safety

Weitere Begriffe, die in Zusammenhang mit Sicherheit im Sinne von Security stehen, sind unter anderem (siehe auch Kapitel 3.1.3): Systemstabilität, Vertraulichkeit und Integrität. Systemstabilität beinhaltet wiederum Verfügbarkeit, Zuverlässigkeit, Safety und Wartbarkeit [TaSt02, S. 362, S. 414]. Somit wird Safety wieder zu einem Unterpunkt von Security.

Verfügbarkeit, Funktionsfähigkeit, Sicherheit (im Sinne von Safety) und Schutz (im Sinne von Security) können wiederum als Ausprägungen oder Eigenschaften der Zuverlässigkeit gesehen werden [Lapr92] bzw. können Safety und Security als zwei Aspekte der Zuverlässigkeit, Verfügbarkeit und Systemstabilität betrachtet werden [StDu98].

Trotz der Unterscheidung von Security und Safety sind beide Eigenschaften untrennbar miteinander verbunden, und beide müssen betrachtet werden, wenn die Sicherheit eines Systems bewertet werden soll.

3.1.2 Safety und Security bei E-Voting

Oft wird bereits bei der Entwicklung von Systemen (man beachte zum Beispiel die Entwicklung von Betriebssystemen) zu wenig auf beabsichtigte Fehler, wie zum Beispiel Angriffe von Hackern, geachtet. Die meisten (vor allem älteren) Arbeiten (z. B. [Barb87, Parh94]), die sich mit Sicherheit von E-Voting auseinander setzten, befassen sich oft nur mit den Facetten der Safety oder Reliability, da sie sich meist nur mit der Vertrauenswürdigkeit des gewählten Prozesses der Stimmabgabe (Wahlprotokoll) beschäftigen, aber weniger mit Problemen bösartiger, beabsichtigter Angriffe.

Beide Facetten sind für die Sicherheit von E-Voting-Systemen relevant, da bösartige Fehler wie auch Unfälle verheerende Folgen für Wahlergebnisse haben können.

3.1.3 Weitere Sicherheitsaspekte

Zuverlässigkeit (*Reliability*) und Safety werden in der Literatur oft gleichgesetzt (vor allem im Bereich der Softwaresicherheit), allerdings ist mit den Begriffen Unterschiedliches gemeint. Mit Reliability ist üblicherweise die Wahrscheinlichkeit gemeint, mit der ein System seinen Zweck unter bestimmten Umständen über eine bestimmte Zeitperiode hinweg erfüllt. Mit Safety hingegen wird in diesem Zusammenhang die Wahrscheinlichkeit bezeichnet, dass Fehler, die zu Unfällen führen, nicht auftreten, unabhängig davon, ob die beabsichtigte Funktion erfüllt wird oder nicht [Leve86, S. 135].

Ian Sommerville definiert Verfügbarkeit und Zuverlässigkeit folgendermaßen:

> „Unter der Verfügbarkeit eines Systems versteht man die Wahrscheinlichkeit, dass das System in der Lage ist, Dienste an seine Benutzer zu liefern, wenn sie gebraucht werden. Unter der Zuverlässigkeit versteht man die Wahrscheinlichkeit, dass die Systemdienste gemäß ihrer Spezifikation ausgeführt werden." [Somm01, S. 369]

Weiters wird zwischen Systemsicherheit und Betriebssicherheit unterscheiden:

> „Die Systemsicherheit eines Systems bewertet das Ausmaß, zu dem sich das System selbst gegen externe Angriffe schützt, die auf Zufall oder Absicht zurückzuführen sind. [..] Die Betriebssicherheit eines Systems ist ein Systemmerkmal, das die Fähigkeit des Systems widerspiegelt, unter normalen wie nicht normalen Umständen zu funktionieren, ohne Menschen oder die Umgebung zu gefährden." [Somm01, S. 369]

Weitere Attribute der Sicherheit, die im Zusammenhang mit Sicherheit von E-Voting-Systemen stehen sind neben Verfügbarkeit (*Availability*), Zuverlässigkeit (*Reliability*), Systemstabilität (*Dependability*), Vertraulichkeit (*Confidentiality*), Integrität (*Integrity*), Wartbarkeit (*Maintainability*) auch: Geheimhaltung (*Secrecy*), Datenschutz (*Privacy*), Transparenz (*Transparency*), Glaubwürdigkeit (*Authenticity*), Fairness (*Fairness*), Eignung (*Eligibility*), Regelbarkeit (*Controllability*), Interoperabilität (*Interoperability*), Prüfbarkeit (*Verifiability*), Nachweisbarkeit (*Auditability*), Verantwortlichkeit (*Accountability*), Barrierefreiheit (*Accessibility*), Genauigkeit (*Accuracy*), Ungezwungenheit (*Non-coercibility*), Zertifizierbarkeit (*Certifiability*), Effizienz (*Efficiency*), Flexibilität (*Flexibility*), Verbraucherfreundlichkeit (*Convenience*), Robustheit (*Robustness*), Bedienbarkeit (*Usability*) und Vollständigkeit (*Completeness*).

All diese genannten Facetten der Sicherheit von Computer-Systemen müssen berücksichtigt werden, um die Sicherheit des Gesamtsystems gewährleisten zu können. Werden verschiedene Facetten von Sicherheit berücksichtigt, wird das Vertrauen in das System gestärkt [HoLa06].

3.2 Gefahr- und Bedrohungstypen

Die Risiken und Gefahren von E-Voting-Systemen sind sehr vielfältig (siehe auch Kapitel 5.4).

Es werden generell vier Typen von Gefahren in IT-Systemen unterschieden [PfPf03, S. 7f]:

- Abfangen (*Interception*): Z. B. ein Unbefugter bekommt Zutritt zum System und kann Nachrichten abhören. Sensible Daten können unerlaubt oder ungewollt kopiert werden.
- Unterbrechung (*Interruption*): Z. B. Daten werden zerstört, gelöscht oder gehen verloren. Eine Einheit des Systems wird unbrauchbar gemacht oder zerstört (z. B. Denial-of-Service Attacke)
- Abwandlung (*Modification*): Z. B. Abänderung von Daten oder Änderung einer Schnittstelle, sodass diese nicht mehr gemäß ihrer Spezifikation funktioniert.
- Herstellung (*Fabrication*): Z. B. Zusätzliche Daten oder Aktivitäten werden erzeugt, die normalerweise nicht bestehen würden.

Diese Punkte können Bedrohungen wie auch Unfälle oder Verluste betreffen und sind somit Safety und Security in selben Maßen zuzuordnen [Leve95, S. 183]. (Security-)Bedrohungstypen lassen sich zudem noch folgendermaßen genauer differenzieren [Hass01, S. 3]:

- Abhören (*Eavesdropping*): Abfangen und Lesen von Nachrichten, die an Andere gerichtet waren.
- Verkleiden (*Masquerading*): Verwendung der Identität eines Anderen zum Senden / Empfangen von Nachrichten.
- Veränderung von Nachrichten (*Message Tampering*): Abfangen und Verändern von Nachrichten, die für Andere bestimmt sind.
- Wiederholung (*Replaying*): Senden einer Nachricht, um Privilegien eines Anderen zu erhalten.
- Infiltrierung (*Infiltration*): Missbrauch eines Anderen Autorität, um feindliche oder bösartige Programme laufen zu lassen.
- Analyse des Verkehrs (*Traffic Analysis*): Observierung des Verkehrs von und zu einem Anderen.
- Service Ablehnung (*Denial-of-Service*): Zugriffsverweigerung auf Ressourcen für Andere.

Die Auslöser für Sicherheitslücken oder Unfälle können sehr unterschiedlich sein. Hauptursachen für (Safety-)Unfälle lassen sich in drei Kategorien unterteilen [Leve95, S. 53]:

- Mängel in der Safety-Kultur der Industrie oder einer Organisation
- Fehlerhafte organisatorische Strukturen
- Oberflächliche oder ineffektive technische Tätigkeiten

Diese Bedrohungstypen ähneln im Wesentlichen denen des STRIDE-Modells [SwSn04, S. 27] (siehe auch Kapitel 3.3.1.1), das folgende Techniken als Gegenmaßnahmen vorschlägt [HoLe02, S. 83ff]:

- Authentifizierung (*Authentication*)
- Autorisierung (*Authorization*)
- Sichere Technologien (*Tamper-resistant and privacy-enhanced technologies*)
- Schutz von Geheimnissen (*Protect secrets, or better yet, don't store secrets*)
- Verschlüsselung (*Encryption, hashes, MACs, and digital signatures (message authentication codes)*)
- Überprüfungen (*Auditing*)
- Überprüfung von Daten (*Filtering, throttling, and quality of service*)
- Niedrigste Rechte (*Least privilege*)

Die verschiedenen Gefahren und Bedrohungen können nach diesen Einteilungen unterschieden, mögliche Ursachen identifiziert und Gegenmaßnahmen vorgeschlagen werden. Diese Kategorisierung hilft, Gefahren und Bedrohungen einzustufen und so auch besser abschätzen zu können. Der weitere Umgang mit Risiken erfolgt durch das Risikomanagement.

3.3 Risikomanagement

Risikomanagement (im Englischen „Risk Management“) bedeutet Erkennen und Begutachten von Risiken und das Entwickeln einer Strategie, um mit diesen Risiken umzugehen. Mit *Risiko* ist hierbei die Wahrscheinlichkeit der Realisierung einer Bedrohung durch Ausnutzung einer Schwachstelle gemeint [PfPf03, S. 22].

Ian Sommerville definiert Risikomanagement folgendermaßen:

„Risk management is concerned with assessing the possible losses that might ensue from attacks on assets in the system and balancing these losses against the costs of security procedures that may reduce these losses." [Somm06, S. 722]

Generell gibt es drei Strategien, um Risiken zu vermeiden [PfPf03, S. 506]:

- Vermeidung des Risikos, indem die Anforderungen an das System geändert werden.
- Transfer des Risikos zu anderen Systemen, Personen oder Organisationen, wie z. B. Durch Abschluss einer Versicherung.
- Akzeptanz des Risikos, indem es über bestimmte Ressourcen kontrollierbar gemacht und der Schaden akzeptiert wird, wenn ein Fehler auftritt.

3.3.1 Risikoanalyse

Die *Risikoanalyse* (im englischen *Threat Modeling*) bietet ein methodisches Vorgehen zur Analyse der Sicherheit eines Computersystems. Mit dieser Methode können Stärken und Schwächen eines Systems aufgezeigt und Schwachstellen gefunden werden [SwSn04, S. 37].

Man beurteilt die Beziehung zwischen der Ernsthaftigkeit der Bedrohung, der Auftrittshäufigkeit (Wahrscheinlichkeit) und den Kosten, um einen passenden Schutzmechanismus einzusetzen. Die Ernsthaftigkeit kann als der Wert gemessen werden, der notwendig ist, um den Schaden einer erfolgreichen Attacke zu reparieren, und wird auch häufig als *Risikolevel* bezeichnet. Der gesamte Prozess wird als Risikomanagement bezeichnet [Hass01, S. 4].

Folgende Schritte sind die Basis des Risikomanagements [EkDa95]:

1. *Identify the assets*: Identifikation der Vermögenswerte
2. *Determine the vulnerabilities*: Bestimmen der Verwundbarkeiten
3. *Estimate the likelihood of exploitation*: Bestimmung der Wahrscheinlichkeit einer Ausnutzung der Sicherheitslücken
4. *Compute the annualized loss expectancy (or alternatively the expected cost of a particular incident)*: Ausrechnen der jährlichen Verlusterwartung (oder Kosten eines einzelnen Vorfalles)
5. *Survey current and possible safeguards*: Betrachtung gegenwärtiger und möglicher Schutzmaßnahmen
6. *Determine the savings according to the safeguards*: Bestimmung der (jährlichen) Ersparnisse durch die Schutzmaßnahmen

Die Assets können in sechs verschiedene Kategorien unterteilt werden [PfPf03, S. 509]: Hardware, Software, Daten, Menschen, Dokumentation, Betriebsmittel (vgl. Kapitel 4.2). Mit Kosten (oder Verlusten) sind generelle Kosten, nicht nur monetäre Verluste, gemeint, wie etwa die Folgen eines Ausfalls, bis hin zu menschlichen Schäden.

Das Problem bei Kosten- und Wahrscheinlichkeitsschätzungen ist, dass man es oft nicht mit exakten Daten, numerisch unpräzisen Wahrscheinlichkeiten und vagen Kosten zu tun hat. Ekenberg und Danielson stellen ein generelles Konzept zum Umgang mit abstrakten Kosten vor [EkDa95], mit dem die Wahrscheinlichkeiten innerhalb von Grenzen oder Kosten als Proportionen angegeben werden können.

Weiters werden *Tree-Problems* (Problembäume) vorgestellt (siehe Abbildung 3), mit denen Zusammenhänge visualisiert werden können. Eine Risikoanalyse wird meist mit einem Entscheidungsbaum [Boeh91], oder auch Attack-Tree oder Fault-Tree dargestellt (siehe Kapitel 3.3.2).

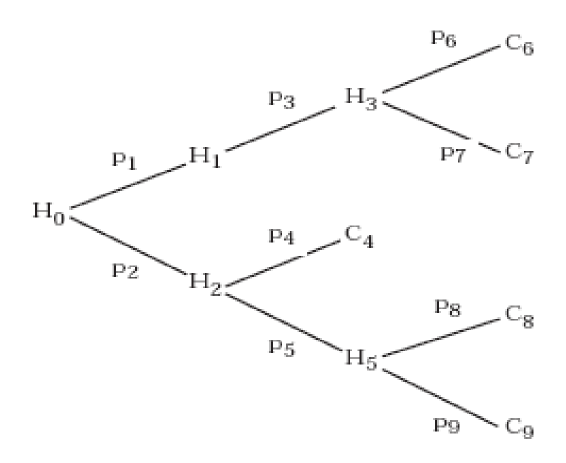


Abbildung 3: Tree-Problem - "An extended consequence analysis". Quelle [EkDa95, S. 10]

Neben den vielen Vorteilen, die die Risikoanalyse mit sich bringt, wie etwa Bildung eines Sicherheitsbewusstseins oder Identifizierung der Vermögenswerte und Schwachstellen, weist sie auch einige Nachteile auf, wie Unflexibilität, fehlende Genauigkeit und Richtigkeit oder hohe Kosten.

3.3.1.1 Das STRIDE-Modell

Eine bekannte Methode für *Threat Modeling* ist das STRIDE-Modell [SwSn04, S. 27], bei dem die Bedrohungen in sechs verschiedene Kategorien eingeordnet werden:

- Vortäuschen einer anderen Identität *(Spoofing identity)*
- Ändern von Daten *(Tampering with data)*

- Nichtanerkennung *(Repudiation)*
- Veröffentlichung von Informationen *(Information disclosure)*
- Zugriffsverweigerung *(Denial-of-Service)*
- Erhöhung der Rechte *(Elevation of privilege)*

Die Schwere der Risiken wird nach DREAD bewertet:

- Schadenspotential *(Damage Potential)*
- Reproduzierbarkeit (Reproducibility)
- Ausnutzbarkeit (Exploitability)
- Betroffene Benutzer (Affected Users)
- Entdeckbarkeit (Discoverability)

Bei STRIDE werden folgende Schritte durchgeführt:

1. Assets identifizieren (z. B. Computer, Daten, etc.), indem Personen aller Interessengruppen (Manager, Entwickler, etc.) befragt werden.
2. Das System durch Data Flow Diagramme abbilden.
3. Assets in STRIDE-Kategorien einordnen.
4. Die Kritizität der Assets mit DREAD bewerten, wobei jeweils ein Wert zwischen 1 und 10 zugeordnet und der Mittelwert kalkuliert wird. Dieser Endwert kann zur Priorisierung der Gegenmaßnahmen verwendet werden.

STRIDE ist eine besonders weit verbreitete Methode, um Bedrohungen zu analysieren, die auch eine Möglichkeit zur Einstufung der Bedrohungen mit numerischen Werten bietet.

3.3.2 Baumanalyseverfahren

Um Risiken oder Kosten und deren Zusammenhänge abzubilden, werden in der Risikoanalyse häufig Baumanalyseverfahren verwendet.

Fault-Tree-Analysen sind ein logischer, strukturierter Prozess, der dabei hilft, mögliche Systemausfälle zu erkennen, bevor sie eintreffen [LeHa83]. Sie wurden ursprünglich 1961 von H. A. Watson der Bell Telephone Laboritories entwickelt und später von Nancy Leveson aufgegriffen. Fault-Tree-Analysen dienen hauptsächlich der Analyse der Ursachen von Risiken, nicht der Identifikation der Risiken selbst. Basis für den Baum sind alle möglichen Ursachen eines Fehlers. Als Wurzelkno-

ten wird der Fehler (*Top Event*) beschrieben, seine Blätter beschreiben Einzelfehler, die diesen Fehler auslösen können. Die Einzelfehler sind wiederum mit Boolscher Logik (Operatoren AND, OR, NOT) verknüpft (siehe Abbildung 4). Jede Ebene des Baumes listet Ereignisse auf, die notwendig sind, um das Ereignis eine Ebene darüber auszulösen [Leve95, S. 317].

Attack-Trees wurden von Bruce Schneier [Schn99; Schn04, S. 309ff] basierend auf Arbeiten zu Fault-Trees von Nancy Leveson [LeHa83; Leve95, S. 317ff] entwickelt. Attack-Trees (siehe Abbildung 5) bieten eine formale Methode, basierend auf unterschiedlichen Attacken, Sicherheit von Systemen zu beschreiben. Ein Attack-Tree repräsentiert einen Angriff auf ein System, dargestellt in einer Baumstruktur. Das Ziel der Attacke ist der Wurzel-Knoten des Baumes, die verschiedenen Arten, dieses Ziel zu erreichen, werden als Blätter-Knoten dargestellt. Je weiter der Knoten sich von der Wurzel entfernt, desto spezifischer wird die Attacke [Schn99].

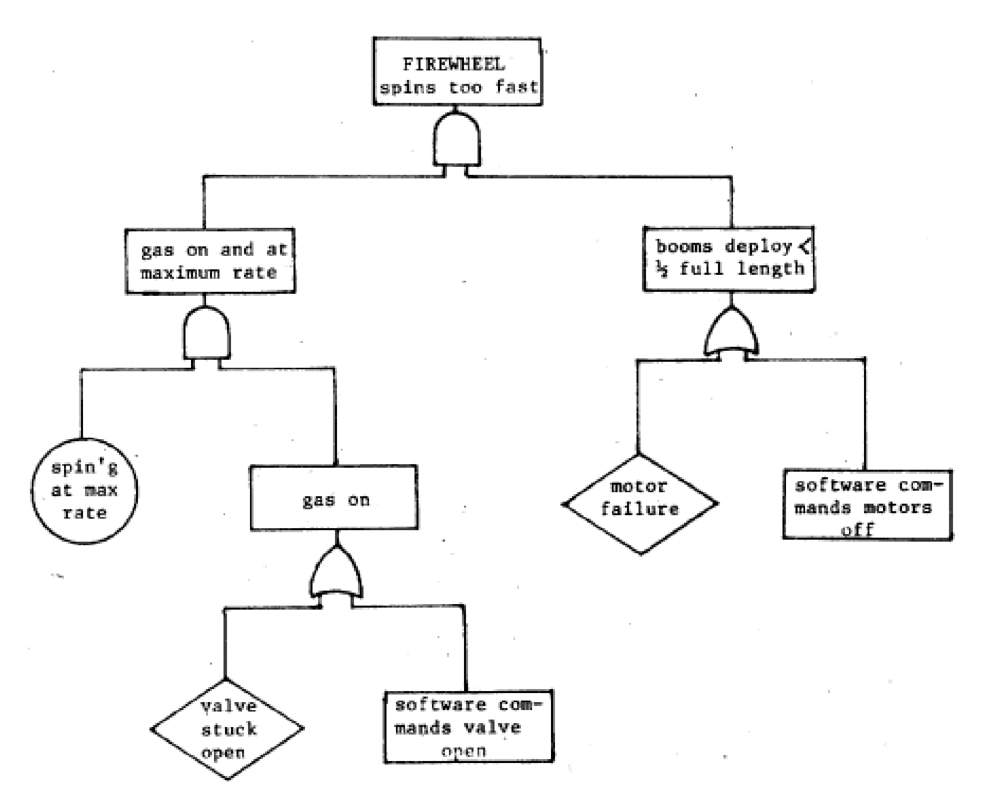


Abbildung 4: Beispiel für einen Fault-Tree. Quelle [LeHa83, S. 571]

Die *Event-Tree-Analyse* [Leve95, S. 327f] ist ein Entscheidungsbaumverfahren, das sich von einem Startereignis zu verschiedenen Folge-Status über eine Reihe möglicher Ereignisse von links nach rechts fortsetzt. Der jeweils nächste Status wird durch den Erfolg oder Misserfolg eines Ereignisses determiniert.

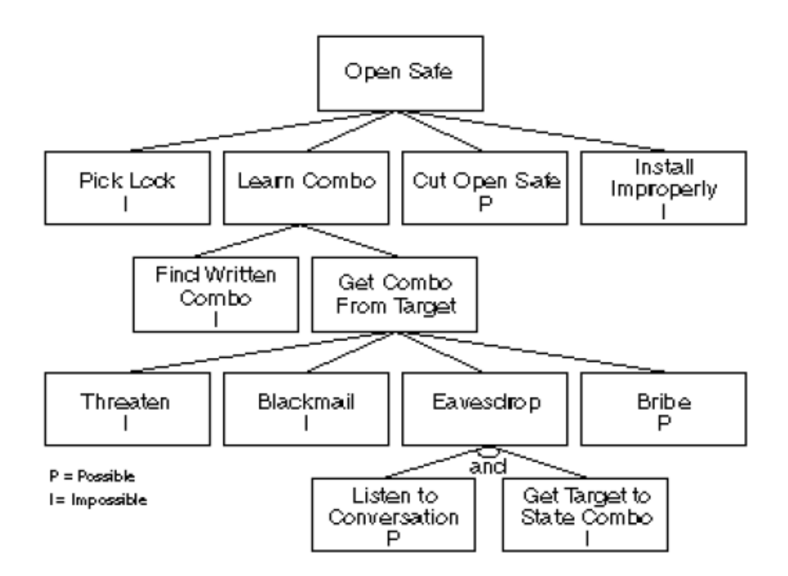


Abbildung 5: Beispiel für einen Attack-Tree. Quelle [Schn99]

Der Nachteil von Baumanalyseverfahren ist, dass sie nur bestimmte Angriffe abdecken und voraussetzen, dass Angreifer ihre Attacken planen und rational abschätzen, ob sich ein Angriff lohnt oder nicht. Mit Attack-Trees werden eine Reihe von Attacken abgedeckt, aber die vollständige Abdeckung eines komplexen Systems kann, auch wegen der Annahme, dass Angreifer vernünftig sind, nicht erreicht werden (vgl. Movie Plot Security Kapitel 5.4.3.6). Eine weitere Schwierigkeit beim Einsatz von Baumanalyseverfahren ist, den Wurzelknoten korrekt zu identifizieren, um eine vollständige Analyse durchführen zu können.

3.3.3 Risikobewertung

Die Auswirkungen von Risiken lassen sich oft nur schwer quantifizieren. Das betrifft zum einen die Bewertung der Auswirkungen bei Eintreten einer Gefährdung und zum anderen die Häufigkeiten von Fehlern oder Sicherheitsbrüchen. Daher bedienen sich verschiedene Organisationen, die Luftfahrtbehörden oder das Militär bestimmter generischer Tabellen, mit deren Hilfe Risiken kategorisiert werden können.

Die zivile Luftfahrt (*Federal Aviation Administration* der USA) verwendet folgende Kategorien zur Risikoeinstufung [FAA03]:

- *Catastrophic:* Fehlerursachen, die mehrfache, fatale Folgen für Fluggäste, die Flugbesatzung oder den Verlust des Flugzeugs mit sich ziehen.

- *Hazardous/Severe-Major*: Fehlerursachen, die die Funktionstüchtigkeit des Flugzeugs stark herabsetzen und die Fähigkeiten der Besatzung, ungünstige Bedingungen zu meistern, stark beeinträchtigen.
- *Major*: Fehlerursachen, die die Funktionstüchtigkeit des Flugzeugs herabsetzen und die Fähigkeiten der Besatzung, ungünstige Bedingungen zu meistern, beeinträchtigen.
- *Minor*: Geringfügige Fehlerursachen, die keinen signifikanten Einfluss auf die Flugzeugsicherheit und auf die Sicherheit der Flugzeugbesatzung haben.
- *No Effect*: Fehlerursachen, die keinen Effekt auf die Sicherheit haben.

Die internationale Norm IEC 61508 *Funktionale Sicherheit sicherheitsbezogener elektrischer/programmierbarer elektronischer Systeme* der International Eletrotechnical Commission (IEC) schlägt ein 4-stufiges System zur Kategorisierung der Konsequenzen von Unfällen vor (siehe Tabelle 1).

Kategorie	***Definition***
Katastrophal	Mehrere Tote
Kritisch	Einzelner Todesfall und / oder mehrere schwere Verletzungen oder Krankheiten der Bewohner
Geringfügig	Einzelne schwere Verletzungen oder Krankheiten der Bewohner und / oder mehrere geringfügige Verletzungen oder geringfügige Krankheiten der Bewohner
Unwesentlich	Einzelne geringfügige Verletzungen oder geringfügige Krankheiten von Menschen

Tabelle 1: Kategorien zur Einteilung der Unfallschwere für militärische Systeme *[Boer04, S. 16] der Norm IEC 61508*

Für die Häufigkeit der Unfälle werden nach dem IEC-Standard sechs Kategorien verwendet (siehe Tabelle 2).

Kategorie	***Definition***
Häufig	Wiederholtes Vorkommen
Wahrscheinlich	Häufiges Vorkommen
Gelegentlich	Könnte irgendwann passieren
Zukünftig	Könnte eines Tages passieren
Unwahrscheinlich	Unwahrscheinlich, doch mit Ausnahmen möglich
Unglaublich	Extrem unmöglich

Tabelle 2: Kategorien zur Einteilung der Unfallwahrscheinlichen für militärische Systeme *[Boer04, S. 20] der Norm IEC 61508*

Eine Klassifizierung des Risikos entsteht durch die Kombination der Werte für Schwere und Häufigkeit der Gefahr. Die Risikoklassifizierung nach IEC 61508 wird in Tabelle 3 mit der *Risk Class Matrix* gezeigt.

	Bedeutung			
Häufigkeit	*Katastrophal*	*Kritisch*	*Geringfügig*	*Unbedeutend*
Häufig	I	I	I	II
Wahrscheinlich	I	I	II	III
Gelegentlich	I	II	III	III
Zukünftig	II	III	III	IV
Unwahrscheinlich	III	III	IV	IV
Unglaublich	IV	IV	IV	IV

Tabelle 3: Risikoklassifizeriung nach IEC 61508 [Boer04, S. 22]

Die vier verschiedenen Klassen werden mit römischen Ziffern nummeriert, wobei Klasse I die mit dem höchsten und Klasse IV die mit dem niedrigsten Risiko darstellt (siehe auch Tabelle 4).

Durch die Einführung von Risikoklassen können Bedrohungen in einige wenige Gruppen eingeteilt werden, für die jeweils eigene Techniken für risikomindernde Maßnahmen angegeben werden. Somit ist es nicht mehr notwendig, für jede Kombination von Häufigkeit und Schwere der Gefahr eine spezielle Sicherheitsfunktion zu entwerfen. Jedes identifizierte Risiko kann somit einer Klasse zugeordnet werden. Die Art und Weise, wie die Bewertung der Risiken erfolgen soll, lässt der Standard offen.

Risikoklasse	*Definition*
I	Inakzeptables Risiko
II	Unerwünscht und nur bei nicht reduzierbarem Risiko oder unverhältnismäßig stark zunehmenden Kosten akzeptabel
III	Tolerierbares Risiko, wenn die Kosten der Risikoreduzierung überschritten werden
IV	Unbedeutendes Risiko

Tabelle 4: Definition der Risikoklassen nach IEC 61508 [Boer04, S. 22]

Das Prinzip, das mit der Risikoklassifikation verfolgt wird, ist Folgendes: Ein Risiko soll so klein wie möglich gemacht werden, wörtlich: „as low as reasonably practicable“. Daraus ergibt sich das ALARP-Prinzip: Das Risiko soll somit so weit reduziert werden, dass die Minimierung noch „preisgünstig“ ist. Die Matrix aus Tabelle 3 gibt auch eine Übersicht, wie Risiken minimiert werden können. So kann ein Risiko der Klasse I in der Kritisch / Wahrscheinlich-Zelle auf Klasse III reduziert werden, wenn seine Wahrscheinlich auf „Zukünftig“, oder seine Konsequenzen auf „Unbedeutend“

oder seine Wahrscheinlich auf „Gelegentlich“ und seine Konsequenzen auf „Geringfügig“ geändert werden. Somit können Sicherheitsanforderungen erstellt werden, die besagen, welche Risiken minimiert werden sollen [Redm98].

Die Grenzen solcher generischer Methoden bestehen darin, dass angenommen wird, dass alle Teile eines meist sehr komplexen Systems erkannt und in der Methode erfasst werden können [FoBe00].

3.4 Technische und prozedurale Sicherheit

Weiters kann zwischen zwei Aspekten der Sicherheit (im Sinne von Security) bei elektronischen Wahlen unterscheiden werden: technische und prozedurale Sicherheit [XeMa04b, XeMa05a]. Bei der technischen Sicherheit wird das Hauptaugenmerk vor allem auf die (technische Umsetzung der) Gewährleistung vollständiger und sicherer Benutzer-Authentifizierung und Wahl-Sicherheit gelegt.

Prozedurale Sicherheit, auf der anderen Seite, behandelt neben technischen Aspekten auch diejenigen, die etwa die Verwaltung und Leitung elektronischer Wahlen betreffen. Hier ist auch der Neuentwurf des Wahlverfahrens oder die Einführung zusätzlicher Aktivitäten oder Mechanismen gemeint, die den Grad an Sicherheit elektronischer Wahlen erhöhen.

Umfassende Arbeiten zum Thema prozedurale Sicherheit wurden bereits veröffentlicht [WeVi07, XeMa04c], einige zeigen Ansätze aus verschiedenen Blickwinkeln, wie etwa einen geografischen Ansatz [HoSt06].

3.5 Informationssicherheit

Informationssicherheit wird oft mit IT-Sicherheit verwechselt. IT-Sicherheit (Schutz vor Viren, Würmern, Hackern, etc.) ist nur ein Gebiet der technischen Sicherheit, welche wiederum mit der physischen und organisatorischen Sicherheit einen der drei wesentlichen Bestandteile der Informationssicherheit als Basis der Sicherheit in Unternehmen bildet.

> „Nur wenn alle drei Komponenten aufeinander abgestimmt sind, ist der Basisschutz für Ihr Unternehmen gegeben.“ [Nagy05]

Im Einzelnen wird nun auf die drei Teilgebiete der Informationssicherheit eingegangen.

Physische Sicherheit, also Sicherheit der Hardware und des Netzwerkes, betrifft unter anderem folgende Punkte:

- Zugangssicherung zu Gebäuden und Räumlichkeiten

- Beobachtungen der Aktivitäten von außen
- Physische Beeinträchtigung der Anlagen, sowohl durch unbeabsichtigte (z. B. Kabelbrand, Wasserrohrbruch, Schäden durch Stürme) wie auch beabsichtigte Schäden (z. B. Auslösen einer Sprinkleranlage)
- Sicherung vor Einbrechern

Technische Sicherheit hat folgende Teilbereiche:

- Betriebssicherheit: z. B. Datensicherung, Zugangssicherheit, Benutzerverwaltung
- Angriffsschutz: z. B. Spionage, Hacker
- Schadprogramme: z. B. Viren, Würmer, Spam
- Entsorgung von Hard- und Software, Datenträgern, Papier, etc. mit geeigneten Datenvernichtern (z. B. Shreddern)
- Outsourcing[21]

Aufgaben der organisatorischen Sicherheit sind:

- Analyse der Gefahrenpotenziale und Gegner
- Unternehmens-Infeld (Mitarbeiter, Social Engineering[22], etc.)
- Unternehmens-Umfeld (Katastrophen, Konkurrenz, etc.)
- Risikomanagement
- Sicherheitsmaßnahmen und Sicherheitsbewusstseins-Schulungen
- Sicherheitsklassifikationen
- Rechtliche Aspekte (z. B. Gesetze, Auflagen, Normen, etc.)
- Sicherheitsorganisation
- Passwortverwaltung / Chipkartenverwaltung
- Katastrophenplanung
- Reaktion auf Vorfälle
- Krisenkommunikation

[21] Outsourcing bedeutet das Auslagern von Teilbereichen.

[22] Social Engineering: Ausnutzen menschlicher Hilfsbereitschaft, um Sicherheitsregeln von Unternehmen zu umgehen.

Diese Aufteilung in physische, technische und organisatorische Sicherheit entspricht in etwa der Aufteilung in Hardware, Software und menschliche Faktoren und Aspekte bzw. *Human Factors*[23] (siehe Kapitel 4.2).

[23] Der Begriff *Human Factors* ist im angelsächsischen Raum extensiver geprägt, als die deutsche Variante „Humanfaktoren“ oder „menschliche Faktoren“. Daher wird in weiterer Folge dieser Begriff als Sammelbegriff für psychische, kognitive und soziale Einflussfaktoren verwendet.

4 E-Voting-Systeme

In diesem Kapitel wird ein allgemeiner Überblick über elektronische Wahlsysteme, deren Teile und Arten gegeben. Es folgt eine Beschreibung der Grundlagen von E-Voting-Systemen (Wahlprotokolle) und ein Überblick über österreichische Entwicklungen und internationale E-Voting-Systeme.

4.1 Definition von Systemen

Folgende Definitionen (vom *Institute of Electrical and Electronics Engineers*) gelten als Abgrenzung zu anderen Bezeichnungen:

Ein *System* wird als Sammlung von Komponenten definiert, die derart angeordnet sind, um spezielle Funktionen oder eine Menge an Funktionen zu vollbringen [IEEE90]. Ein *Softwaresystem* ist ein System, für das Software die einzige entwickelte oder änderbare Komponente ist [IEEE98]. Ein *Informationssystem* ist ein Mechanismus, der Informationen handhabt (Erfassung, Ablage, Speicherung, Wiedergewinnen) [IEEE90].

Ein *E-Voting-System* ist ein System, das aus mechanischen, elektromagnetischen oder elektronischen Teilen besteht. Es beinhaltet Software zur Steuerung der Geräte, zur Definition der Stimmzettel, zum Abgeben und Zählen der Stimmen und zur Erstellung und Darstellung der Ergebnisse [FEC01, Volume I, Section 1, 1-4]. Mit einem E-Voting-System wird ein Teil des Wahlvorgangs elektronisch abgebildet. So werden etwa die Stimmzettel auf elektronischem Weg ausgedrückt oder gezählt (vgl. Kapitel 1.3).

4.2 Teile eines E-Voting-Systems

Die Definition von (allgemeinen) Systemen nach Eberhardt Rechtin besagt:

> „A system is a construct or collection of different elements that together produce results not obtainable by the elements alone. The elements, or parts, can include people, hardware, software, facilities, policies, and documents; that is, all things required to produce systems-level results. The results include system level qualities, properties, characteristics, functions, behavior and performance. The value added by the system as a whole, beyond that contributed independently by the parts, is primarily created by the relationship among the parts; that is, how they are interconnected." [Rech99, S. 4]

Eine weitere Definition (vom *International Council on Systems Engineering*) beschreibt ein System folgendermaßen:

„A system can be broadly defined as an integrated set of elements that accomplish a defined objective.“ [INCO00]

Ein System dient somit der Erfüllung einer bestimmten Aufgabe und besteht aus Elementen (Teilen / Komponenten), wobei damit in einem sehr allgemeinen Sinne die Bausteine des Systems gemeint sind. Elemente können wiederum als Systeme betrachtet werden [DaHu92, S. 5].

Ein sicherheitsbezogenes System[24] wird von der *International Eletrotechnical Commission* IEC folgendermaßen definiert:

„A safety-related system comprises everything (hardware, software and human elements) necessary to carry out one or more safety functions, where failure of the safety function would give rise to a significant increase in the risk to the safety of persons and/or the environment.“[25]

Ian Sommerville unterscheidet drei „Systemkomponenten“ kritischer Systeme, in denen Ausfälle auftreten können [Somm07, S. 73]:

- Systemhardware
- Systemsoftware
- Menschliche Bediener des Systems

Die identifizierten sicherheitsrelevanten **Elemente eines E-Voting-Systems** sind somit Folgende:

- *Hardware*: Hier wird zwischen mechanischen und elektronischen Teilen unterschieden.
- *Software*: Betriebssystem, Treiber, Compiler, Programme, Datenbanken, im Programm verwendete Regeln, Prozeduren und Abläufe (Verlauf der Stimmabgabe, Wahlprotokoll).
- *Human Factors*: In diese Kategorie fallen Usability, organisatorische Aspekte, angewandte Richtlinien und Strategien (etwa Informationsweitergabe oder Handhabung von Passwörtern), Politik und andere Aspekte wie etwa Akzeptanz.
- *Schnittstellen*: Weitere sicherheitsrelevante Elemente sind die Verbindungen bzw. die Schnittstellen zwischen den oben beschriebenen Komponenten (Schnittstellen Hardware-Software,

[24] Eine formale Definition eines sicherheitsbezogenen Systems ist in IEC/EN 61508 Teil 4, Abschnitt 3.4.1 zu finden.

[25] Von der Homepage des IEC http://www.iec.ch/zone/fsafety/concepts.htm

Hardware-Mensch und Software-Mensch) und den Teilen der Komponenten untereinander (Schnittstellen Hardware-Hardware, Software-Software und Mensch-Mensch). Beispiele für Schnittstellen sind das Internet (Hardware-Hardware) oder die grafische Benutzerschnittstelle (Software-Mensch).

Jeder Teil eines Systems solle als gleich bedeutend in Hinblick auf Sicherheitsrisiken betrachtet werden, wobei die Schnittstellen den drei Hauptelementen (Hardware, Software und Human Factors) zugeordnet werden (siehe auch Kapitel 5.4).

Grundlegend für E-Voting-Systeme ist die Einhaltung der Wahlgrundsätze (siehe Kapitel 2):

- Allgemeines Wahlrecht: Jeder darf wählen
- Freies Wahlrecht: Entscheidungsfreiheit
- Gleichheit: ein Stimmzettel pro Wähler
- Unmittelbares Wahlrecht: Ohne Wahlmänner in einer Runde wählen[26]
- Geheimes Wahlrecht: Anonymität
- Persönliches Wahlrecht: Ohne Stellvertreter persönlich wählen
- Verhältniswahlrecht: Auszählungsart[27]
- Öffentlichkeit und Transparenz

Die Einhaltung des freien, geheimen und persönlichen Wahlrechts und der Transparenz ist in Bezug auf E-Voting besonders umstritten. Die Umsetzung des unmittelbaren Wahlrechts und des Verhältniswahlrechts obliegt nicht direkt dem elektronischen System, sondern der Wahlorganisation. Werden die Wahlgrundsätze nicht eingehalten, ist die Integrität des Demokratieprozesses gefährdet, was einem *Single Point of Failure*[28] gleich kommt. Das gesamte E-Voting-System ist als unbrauchbar einzustufen, wenn nur einer dieser Wahlgrundsätze nicht eingehalten wird.

Basis für ein elektronisches Wahlsystem ist das etablierte Wahlverfahren im jeweiligen Land, in dem das System eingesetzt werden soll (siehe auch Kapitel 2.2). Ein E-Voting-System sollte an die bisherige Systematik so weit wie möglich angelehnt sein, alle rechtlichen Aspekte abdecken und das System durch zusätzliche Sicherheit und Transparenz ergänzen.

---

[26] Wahlen mit Stellvertretern könnten durch ein E-Voting-System gelöst werden, indem verschiedene Personenkreise in mehreren Phasen wählen würden.

[27] Ein Mehrheitswahlrecht kann durch ein elektronisches System ebenfalls realisiert werden, indem das Ergebnis dementsprechend interpretiert werden würde.

[28] Der Ausfall einer einzelnen speziellen Komponente zieht den Ausfall des Gesamtsystems nach sich.

4.3 Überblick über E-Voting-Systeme

Bei E-Voting-Systemen wird das Hauptaugenmerk meist auf das formale *Wahlprotokoll* (auch *Wahlalgorithmus* oder *Wahlschema* genannt, siehe auch Kapitel 4.4), also die Architektur (etwa eine Trennung von Wählerevidenz und Wahlurne) und die Schritte des Ablaufs der Stimmabgabe gelegt.

Die Hauptaufgaben von E-Voting-Systemen sind [Schl00, S. 11; CrCy97]:

- Registrierung der Benutzer (Wählerevidenz)
- Validieren der Wähler: Identifizierung, Authentifizierung, Autorisierung
- Darstellung des Stimmzettels und Abgabe der Stimme
- Sammlung der Stimmzettel
- Auswertung der Stimmzettel und Darstellung eines Wahlergebnisses

Anschließend ist eine Auditing-Phase nach der Wahl sinnvoll [MeNe03a]. In dieser Phase wird etwa überprüft, ob nur berechtigte Wähler gewählt haben, nur Stimmen Berechtigter im Gesamtergebnis enthalten sind oder die Stimmen, die abgegeben wurden, auch tatsächlich so im Wahlergebnis enthalten sind, wie sie vom Wähler bestimmt wurden (siehe auch Kapitel 6.7.2).

4.3.1 Ausprägungen von E-Voting

Unter dem Begriff *E-Voting* (basierend auf der Definition in Kapitel 1.3) vereinen sich eine Reihe von Systemen in verschiedenen Ausprägungen. E-Voting-Lösungen sind etwa Software-Gesamtlösungen (*E-Voting-Systeme*, gemäß Definition in Kapitel 4.1), bei denen von der Registrierung bis zur Stimmenauswertung alle Schritte elektronisch abgebildet werden (z. B. *Direct Recording Electronic* (DRE) Maschinen, ein Beispiel für eine solche Maschine wird in Abbildung 6 gegeben) oder Internet-Wahlsysteme.



Abbildung 6: Touchscreen-E-Voting-Computer vom Hersteller Diebold. Quelle Wikipedia.org http://en.wikipedia.org/wiki/Voting_machine

Weiters wird auch der Einsatz von Hilfsmitteln, bei denen die Stimmen der Wähler auf elektronischem Weg repräsentiert oder gesammelt werden, zum Bereich E-Voting gezählt. Beispiele sind optische Scanner, mit denen Papierstimmzettel nach der Stimmabgabe eingelesen und digital weiterverarbeitet werden (*E-Counting*), Lochkartensysteme (*Punch Card Systems* oder auch *Prescored Punch Cards* (PPC) genannt), bei denen die gestanzten Karten ebenfalls elektronisch / optisch gescannt werden (auch *Optical Mark-Sense Voting Systems* genannt, siehe Abbildung 7), oder Hebelmaschinen (*Lever Voting Machines*), bei denen die Stimmen über mechanisch / elektronischen Weg abgegeben und elektronisch gezählt werden.



Abbildung 7: Optischer Scanner für Lochkarten. Quelle http://americanhistory.si.edu/vote

Es gibt eine Reihe von Herstellern, die verschiedenste E-Voting-Systeme unterschiedlichster Ausprägungen und auf Basis unterschiedlichster Technologien und Ansätze herstellen. Derzeit gibt es weder in den USA, noch in Europa einheitliche Standards, die verpflichtende Richtlinien für die Entwicklung elektronischer Wahlsysteme bereitstellen (siehe auch Kapitel 6.8).

4.3.2 E-Voting im Einsatz

E-Voting im Wahllokal ist in einigen Ländern (z. B. Belgien, Holland, USA, Russland, Brasilien) bereits übliche Praxis, in Einzel- bzw. Testfällen z. B. auch in Deutschland, Kanada, Portugal, Dänemark und Australien. In anderen Ländern wird E-Voting evaluiert (z. B. Portugal, Finnland, Mexiko, Österreich) [Buch04].

Die ersten E-Voting-Systeme wurden in den 1960er Jahren in den USA eingesetzt. Damals wurden Lochkartensysteme und Wahlcomputer in einigen Staaten verwendet. Das erste Land, das den Wahlprozess bei rechtsgültigen Wahlen durch Wahlmaschinen unterstützen ließ, war Brasilien. Bereits 1996 liefen Tests mit einer eigens entwickelten Maschine (siehe Abbildung 8). Seit 1998 beteiligt sich die Firma Diebold[29] ebenfalls an dem brasilianischen Projekt. Seit 2000 werden nur noch elektronische E-Voting-Systeme eingesetzt (über 40.000 Wahlkioske), seit 2002 gibt es zusätzlich Papierbelege [Reze04].

[29] Diebold Election Systems, Inc. (DESI), eine Tochtergesellschaft von Diebold, wurde in „Premier Election Solutions“ umbenannt.



Abbildung 8: Brasilianische Wahlmaschine. Quelle: http://derStandard.at

Belgien genehmigte E-Voting per Gesetz 1994 und setzte bereits 1999 und 2000 elektronische Systeme ein. Rund 44 % aller belgischen Wähler gaben 2000 ihre Stimme elektronisch ab. Dabei wurde bei den PC-basierten Systemen *Digivote* von Steria und *Jites* der Firma Stesud die Stimme auf einer Magnetstreifenkarte gespeichert [OSCE07].

In den USA wurden erstmals im Jahr 1992 DRE-Wahlmaschinen eingesetzt [Salt06, S. 164]. Davor war das amerikanische Volk bereits an Lochkartensysteme und Hebelmaschinen (seit 1929 [Salt06, S. 156]) gewöhnt. Es ergaben sich eine Reihe von Problemen durch den Einsatz dezentralisierter, heterogener Systeme. Abbildung 9 zeigt die damals erwartete Aufteilung der eingesetzten verschiedenen Wahlsysteme in den USA 2004. E-Voting-Systeme (inklusive optischer Scanner) wurden zu knapp zwei Drittel eingesetzt, Papierstimmzettel zu unter einem Prozent.

Expected Voting Equipment Usage in 2004

Punch Card	(Includes DataVote) 13.75%
Lever	13.91%
Paper Ballot	.66%
Optical Scan	33.72%
Electronic	30.75%
Mixed	7.22%

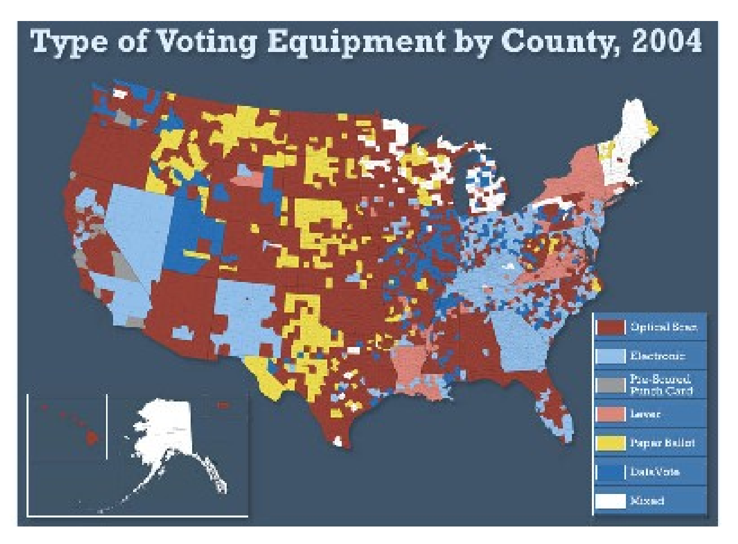


Abbildung 9: Aufteilung der verschiedenen Wahlsysteme in den USA 2004. Quellen: Election Data Services Inc. survey, as of May 4, 2004 und http://americanhistory.si.edu/vote

Neben den kommerziellen DRE-Touchscreen E-Voting-Systemen von Diebold *AccuVote-TS* und *AccuVote-TSX* (siehe auch Abbildung 10), wurden auch die DRE-Systeme von Sequoia wie *WinEDS* oder *AVC Edge, WinVote* von Advanced Voting Solutions, Inc., *iVotronic* von Election Systems & Software (ES&S), *eSlate* von Hart Intercivic, Geräte von *MicroVote* und anderen Herstellern in den USA eingesetzt. Neben DRE-Systemen wurde bisher noch das optische Scan-Wahlsystem *InkaVote Plus* von ES&S verwendet.

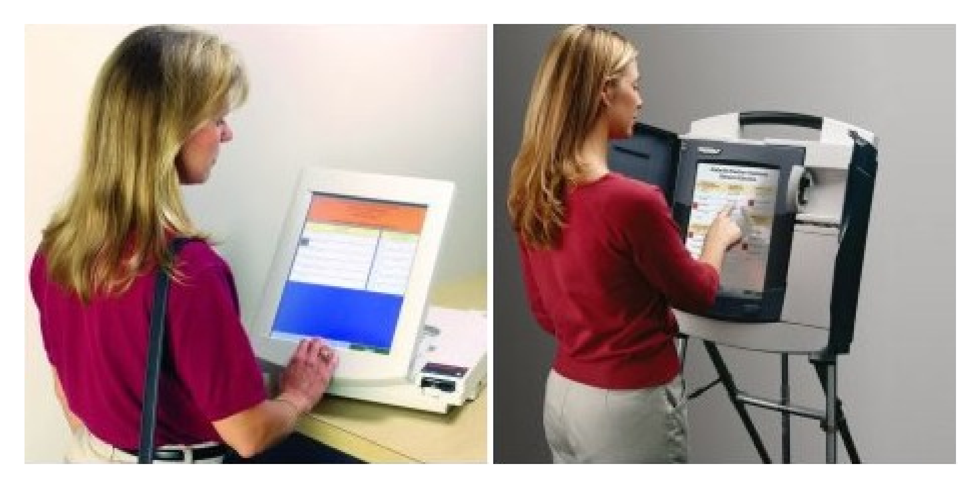


Abbildung 10: Diebold Wahlmaschinen AccuVote-TS und AccuVote-TSX. Quelle: www.premierelections.com

In Deutschland stimmten bei der Bundestagswahl 2005 etwa 2,5 Millionen Wähler in 2.100 von insgesamt 80.000 Wahllokalen elektronisch ab [Siet05]. Ein eher älteres Modell wurde bei den Landtagswahlen im Saarland, Deutschland, 2004 eingesetzt (siehe Abbildung 11).



Abbildung 11: Maschine, die bei den Landtagswahlen im Saarland 2004 eingesetzt wurde. Quelle: http://derStandard.at

Bei der Wahl im Mai 2006 in Italien wurden in den Regionen Liguria, Lazio, Sardinien und Puglia parallel zum traditionellen Verfahren Wahlmaschinen (siehe Abbildung 12) zu Testzwecken eingesetzt.



Abbildung 12: Test-Maschine in Italien. Quelle: http://derStandard.at

Nachdem es bei den italienischen Parlamentswahlen im April 2006 zu einem Verschwinden von rund 700.000 nicht ausgefüllten Stimmzetteln kam und der Verdacht auf eine fehlerhafte Erfas-

sung bei der manuellen Übertragung auf Zähl-PCs fiel, stellte Innenminister Giuliano Amato weitere E-Voting-Versuche in Italien ein[30].

In Indien gab es bereits im Jahr 1999 Tests mit E-Voting-Systemen [Beno04]. Erstmals kamen elektronische Wahlmaschinen zu landesweite Wahlen 2004 (siehe Abbildung 13) zum Einsatz [KaKa05]. Da etwa ein Drittel der Indischen Bevölkerung Analphabeten sind, wurden neben der textuellen Beschreibung der Partei auch das Symbol dieser daneben angezeigt.



Abbildung 13: Indische Wahlmaschine. Quelle: http://derStandard.at

Bei den Parlamentswahlen in Estland im März 2007 war auch eine Stimmabgabe über das Internet (von einem PC aus, mit einer ID-Karte und Lesegerät) im Voraus möglich. Drei Prozent der rund 895.000 Wahlberechtigen haben ihre Stimme auf diese Weise nach dem Private/Public-Key-Verfahren abgegeben. Um Beeinflussung zu verhindern, war es möglich, die elektronisch abgegebene Stimme durch den herkömmlichen Urnengang mit einem Papierstimmzettel wieder zu stornieren. Die zuvor elektronisch abgegebene Stimme wurde nicht in das Wahlergebnis übernommen, sondern durch die Stimme auf dem Papierstimmzettel ersetzt. Weiters war es möglich, die Stimme mehrmals hintereinander von verschiedenen Orten aus elektronisch abzugeben, wobei nur die letzte abgegebene Stimme gezählt wurde. Die estländische Regierung wollte mit multiplen Stimmenabgaben die Probleme des Stimmenkaufs und des Wahlzwanges umgehen [VoGr06]. Bereits 2005 war E-Voting in Estland möglich. Bei den Kommunalwahlen 2005 wählten zwei Prozent der Wähler elektronisch [MaMa06].

[30] Quelle: Bericht „Elections: Amato, stop to electronic voting“ der italienischen Nachrichtenagentur AGI.

In der Schweiz wurden seit 2002 mehrere E-Voting-Pilotversuche im Rahmen des Projekts *Vote Èlectronique* in den Kantonen Genf, Neuenburg und Zürich mit verschiedenen E-Voting-Verfahren (auch Wählen über Internet oder per SMS) für Wahlen und Abstimmungen durchgeführt [BrBr06]. Das Projekt gewann den *Public Service Award 2007* der Vereinten Nationen. Durch die Häufigkeit der Wahlen (in häufigem Abstand stehen regionale Entscheidungen mehrmals pro Jahr zur Wahl) sank die Wahlbeteiligung in den letzten Jahren. Mit Einsatz der neuen elektronischen Systeme soll die Wahlbeteiligung wieder gehoben werden. In Zürich sind derzeit rechtsgültige Wahlen per Internet[31] möglich.

Australien verwendet ein Open-Source E-Voting-System basierend auf Linux, das erstmals 2001 bei den Australian Capital Territory Wahlen seinen Testlauf hatte. Das System *Electronic Voting and Counting System* (kurz eVACS[32] genannt) wurde von einer privaten Firma nach staatlichen Richtlinien entwickelt. Der Sourcecode dieses Systems wurde der Öffentlichkeit im Internet unter der GPL[33] verfügbar gemacht. Obwohl bei diesem System keine Papierbelege verwendet werden, gab es eine Reihe positiver Reaktionen auf die offene Entwicklung und die Bewertung durch unabhängige Parteien, die zur Zerstreuung der Kritik an diesem System beitrugen.

In Frankreich wurden in der ersten Runde der Präsidentschaftswahlen 2007 in einigen Städten als Pilotversuch DRE-Maschinen ohne Papierbelege eingesetzt. Es kam zu Zwischenfällen, die einige politische Parteien als „Katastrophe" bezeichneten, wie lange Warteschlangen, Computerstörungen und Ausfälle in einigen Städten (Amiens, Ifs, Le Perreux und St Malo), worauf die politischen Akteure eine Zurückziehung bei der zweiten Runde der Wahl forderten. In Frankreich wurden die DRE-Geräte *Point&Vote* des spanischen Herstellers Indra und Wahlcomputer der Hersteller Nedap und ES&S eingesetzt [Engu06].

In Irland wurde die landesweite Einführung von E-Voting 2002 mit Nedap-Wahlcomputern für die Europawahlen 2004 vorbereitet, doch nach Bürgerprotesten und dem erfolgreichen Kampf der *Irish Citizens for Trustworthy E-Voting ICTE*[34] kam es nie zur tatsächlichen Durchführung einer elektronischen Wahl, obwohl die Nedap-Wahlgeräte bereits für 51 Millionen Euro beschafft worden waren.

In England wurden zahlreiche Pilotversuche zu E-Voting durchgeführt, allerdings sprach sich die englische *Electoral Commission*, die parlamentarisch eingesetzte Wahlaufsichtsbehörde, im August 2007 gegen weitere E-Voting-Pilotversuche mit Internet- und Telefonwahlen aus. Weiters wies die

[31] Internetwahlen für den Kanton Zürich https://evoting.zh.ch

[32] http://www.elections.act.gov.au/elections/electronicvoting.html

[33] Die GNU General Public License (GPL) wurde von der Free Software Foundation mit Copyleft (unbeschränktes Verändern oder Kopieren) für die Lizenzierung „freier" Software herausgegeben.

[34] http://evoting.cs.may.ie

Kommission auf die extrem hohen Kosten (umgerechnet 150-900 Euro pro Stimme) hin, was die Argumente der Befürworter für Kostenreduktion durch den Einsatz von E-Voting entkräftete (siehe auch Kapitel 1.3.1).

4.3.3 Internet-Wahlsysteme

Trotz des kategorischen Ausschlusses von I-Voting-Systemen (für nationale Wahlen, da Internet-Wahlverfahren als inhärent unsicher gelten, siehe Kapitel 1.4) wird hier ein kurzer Überblick über akademische Projekte und kommerzielle Lösungen dieser Art von Systemen gegeben.

Zu Internetwahlen gab es eine Reihe staatlicher, wie auch privater Pilotversuche (z. B. in Frankreich, Italien, Dänemark, Portugal, Deutschland). In einigen Staaten (z. B. in England, Schweiz, Japan, Holland und Spanien) wurden auch Echtwahlversuche durchgeführt [BMI04]. Neben einigen Pilotversuchen in den USA [Hoff00] fand die erste rechtlich bindende Wahl über das Internet bei den Primary-Präsidentschaftswahlen in Arizona, USA, im März 2000 statt [MoGl01]. Die ersten rechtsgültigen nicht-politischen Wahlen fanden im Februar 2000 bei den Wahlen des neuen Studentenparlaments in Osnabrück statt [KaRu03].

SERVE (*Secure Electronic Registration and Voting Experiment*) ist ein von der Firma Accenture im Rahmen eines Pentagon-Programmes der USA hergestelltes Internet- und PC-basierendes DRE-Wahlsystem, das 2004 durch eine Peer-Review Group vor dem Einsatz examiniert wurde. Dieses System sollte die bis dahin papierbasierten Auslandswahlkarten (*Absentee Ballots*) für Amerikaner außerhalb der Heimat (vor allem Soldaten) durch ein I-Voting-System ersetzen. Bei der Untersuchung des Wahlsystems durch einige anerkannte Sicherheitsexperten wurden allerdings grobe Sicherheitsmängel aufgezeigt, sodass es nie zu einem Einsatz des Systems kam [JeRu04].

Eines der Resümees der Analyse stammt von Prof. Aviel Rubin:

> „It's not possible to create a secure voting system with off-the-shelf PCs using Microsoft Windows and the current Internet." [Keat04]

Ein anderer Kommentar zur Entscheidung des U.S. Militärs das Wahlsystem doch nicht einzusetzen, kam von Andrew W. Appel von der Princeton Universität:

> „As an expert in computer security and in voting technology, I believe that this was a wise decision." [Appe06a]

T-Systems entwickelte das Internetwahlsystem *T-Vote*, das 2002 [TSys08], 2005 und 2006 [move05] bei internen Betriebsratswahlen der T-Systems Deutschland eingesetzt und bei der Wahl zum Oberbürgermeister in Trier am 24. September 2006 in einem Wahlbezirk parallel zur Urnenwahl getestet wurde.

i-vote[35] ist ein Internetwahlsystem der Stiftung Internetwahlen von der deutschen Universität Osnabrück. Es basiert auf digitalen Signaturen (siehe auch Kapitel 4.4.1) und kann auf CD mit dem i-voteX Live-Betriebssystem ausgeliefert werden.

Im Rahmen des dreijährigen EU-Projekts Cybervote[36], das von 2001 bis 2004 lief, wurde ein Prototyp für Internetwahlen in Zusammenarbeit mit der Firma EADS erstellt. Mit diesem Wahlsystem konnte von jedem beliebigem Betriebssystem aus über einen Browser oder über ein Mobiltelefon mit einem Java Client gewählt werden. Das Internetwahlsystem sollte bei den französischen Präsidentschaftswahlen 2007 eingesetzt werden, allerdings wurde eine Verletzung des geheimen Wahlrechts entdeckt. In jedem Land wurde eine Liste der Wähler und eine Liste der abgegebenen Stimmen geführt. Da durch die Verteilung in einigen Ländern aber nur wenige Personen abstimmten, hätte man die Stimme bestimmten Personen zuordnen können. Der Einsatz wurde abgebrochen [Appe06a].

Das Internetwahlsystem *Polyas*[37] wurde von der Micromata GmbH entwickelt und lässt rechtsverbindliche Online-Wahlen für Vereine und Verbände abwickeln. So werden etwa die Präsidiumswahlen der Gesellschaft für Informatik über dieses System durchgeführt.

Frühe kommerzielle Internetwahlsysteme aus den 90er Jahren sind *Sensus* [CrCy97] von Lorrie Cranor (siehe auch Kapitel 4.4.1.1) und *E-Vox*. Das E-Vox Internetwahlsystem wurde am *Massachusetts Institute of Technology* MIT unter der Aufsicht von Ronald Rivest basierend auf der Arbeit von Mark Herschberg entwickelt [Hers97]. Das System wurde in Java geschrieben und bei einer Studentenvertretungswahl am MIT 1999 verwendet.

Die japanische Mitarbeiterin Kazue Sako der Firma NEC entwickelte das I-Voting-System *Secure Voting in Symposiums* (SIVS), mit dem bei Konferenzen über die besten eingereichten Arbeiten abgestimmt werden kann.

Adder ist ein freies und offenes Internetwahlsystem, das von Mitarbeitern der University of Connecticut unter der Leitung von Aggelos Kiayias für die Linux Distribution Ubuntu entwickelt wurde [KiKo06]. Der Sourcecode ist auf der Projekthomepage[38] zum Download frei verfügbar.

---

[35] http://www.i-vote.de

[36] http://www.eucybervote.org

[37] http://www.micromata.de/produkte/polyas.jsp

[38] http://cryptodrm.engr.uconn.edu/adder

Das *Condorcet Internet Voting Service* (CIVS) ist ein Wahlsystem für viele Formen von Abstimmungen, wie zum Beispiel von Buchclub-Auswahlen, das mehr in Richtung Reihen von Präferenzen geht. Das I-Voting-System ist unter der Leitung von Andrew Myers an der Cornell Universität entstanden.

Die Europäische Kommission startete im Rahmen des IST (Information Society Technology) Programmes das Projekt e-VOTE[39], ein Forschungs- und Endwicklungsprojekt, das 2001 begonnen wurde und 2,5 Jahre andauerte. Das Resultat waren einige Publikationen (z. B. [MiGr02, LaGr02]), wie auch ein Prototyp für Internetwahlen.

4.4 Wahlprotokolle

Es gibt eine Reihe unterschiedlicher Wahlprotokolle (auch Wahlschema oder -algorithmus genannt), die die Basis von E-Voting-Systemen formen. Wahlschemata bilden die mathematische Grundlage elektronischer Wahlen, wie etwa die Kryptografie bei sicherer Übertragung. Diese Protokolle bilden den Wahlvorgang, also den Weg von der Registrierung, über die Stimmabgabe, bis hin zur Auszählung und Bekanntgabe des Endergebnisses, ab.

In diesem Kapitel wird ein Überblick über die Entwicklung der verschiedenen Wahlschemata gegeben.

4.4.1 Blinde Signaturen

Ein Problem bei der Verwendung digitaler Übertragung ist, dass mit gängigen Methoden nachvollzogen werden kann, wer welche Stimme abgegeben hat. Das von David Chaum 1982 entwickelte und vorgestellte Verfahren der blinden Signaturen [Chau82] behebt dieses Problem, indem es authentifizierte Stimmen zulässt, ohne den Sender zu enthüllen.

Das mathematische Verfahren, basierend auf digitalen Signaturen nach dem *Public Key Encryption* Verfahren [DiHe76], das zugleich Authentizität und Anonymität sichert, wird anhand einer von Chaum verwendeten Analogie mit einem Blaupause-Briefkuvert erklärt: Das zu signierende Dokument wird in ein Blaupause-Briefkuvert gesteckt und der Absender unterschreibt auf dem Kuvert, ohne dessen Inhalt zu kennen. Die Signatur drückt sich auf den Dokumentinhalt durch und dieser wird somit signiert, ohne dass der Unterschreiber diesen je gesehen hat.

Nach der blinden Signatur kann, ohne dass der Unterschreiber den Inhalt des Kuverts entziffern konnte, die Gültigkeit der digitalen Unterschrift durch den öffentlichen Schlüssel des Signierenden überprüft werden.

Folgende Schritte werden bei diesem Verfahren angewandt:

[39] http://www.instore.gr/evote

- Die Nachricht von Absender A, die blind unterschrieben werden soll, wird durch m dargestellt. Die öffentlichen und privaten Schlüsselpaare (e, n) und (d, n) des Signierenden B werden für diesen Vorgang benötigt.
- A erzeugt eine beliebige Zufallszahl r, den sogenannten *Blindingfaktor*, der mit dem öffentlichen Schlüssel n des Empfängers kodiert wird: $r^e \bmod n$ [40]. Die Nachricht wird mit diesem Schlüssel durch Multiplikation verschlüsselt und man erhält $m * (r^e \bmod n)$.
- Die verschlüsselte, von B nicht lesbare Nachricht wird nun an B geschickt, der sie mit seinem privaten Schlüssel signiert $[m * (r^e \bmod n)]^d \bmod n$ und wieder zurück an A schickt.
- Die signierte codierte Nachricht $[m * (r^e \bmod n)]^d \bmod n$ kann nun mit der Modulo-Inversen des Blindingfaktors $r\text{-}1$ multipliziert werden und A erhält die von B signierte Nachricht $m^d \bmod n$, da die folgende Bedingung für das Codieren und Decodieren gilt: $(r^e \bmod n)^d \bmod n = r$.

Somit kann mit diesem relativ simplen mathematischen Verfahren erreicht werden, dass der Sender A eine vom Signierenden B digital signierte Nachricht erhält, ohne dass B den Inhalt der Nachricht lesen konnte und die Nachricht somit geheim bleibt.

Blinde Signaturen kommen bei vielen E-Voting-Verfahren zum Einsatz, da sie Authentizität und gleichzeitig Anonymität elektronischer Stimmzettel gewährleisten.

4.4.1.1 Verfahren nach Fujioka et al

Viele der gängigen E-Voting-Verfahren basieren auf dem Wahlprotokoll von Fujioka et al, das 1993 erstmals in [FuOk93] publiziert wurde. Das Protokoll arbeitet mit (normalen) digitalen und blinden Signaturen und verlangt, wie die meisten E-Voting-Systeme, anonyme Kanäle. Digitale Signaturen basieren auf asymmetrischer Verschlüsselung, bei der ein Schlüsselpaar verwendet wird, dasaus einem öffentlichen und einem privaten Schlüssel besteht. [Pipe97] (siehe auch Kapitel 4.4.1).

Das Wahlprotokoll hat drei verschiedene Akteure:

- Administrator (Authentifizierungsserver)
- Zähler (Urnenserver)
- Wähler

[40] Die Modulo-Operation *mod n* beschreibt den Restwert einer Division durch *n*.

Die Sicherheitsannahme dieses Wahlverfahrens besteht darin, dass ein System sicher ist, wenn es folgende Punkte erfüllt:

- *Completeness* (Vollständigkeit): Alle gültigen Stimmen werden korrekt gezählt.
- *Soundness* (Zuverlässigkeit): Ein „unehrlicher“ Wähler kann die Wahl nicht gefährden.
- *Privacy* (Privatsphäre): Alle Stimmen sind geheim.
- *Unreusability* (keine Wiederverwendung): Kein Wähler kann doppelt wählen.
- *Eligibility* (Eignung): Keiner, der nicht wählen darf, kann wählen.
- *Fairness* (Gerechtigkeit): Nichts beeinflusst die Wahl.
- *Verifiability* (Prüfbarkeit): Niemand kann das Wahlergebnis fälschen.

Das Protokoll sieht folgende sechs Schritte bei der Stimmabgabe vor (siehe Abbildung 14):

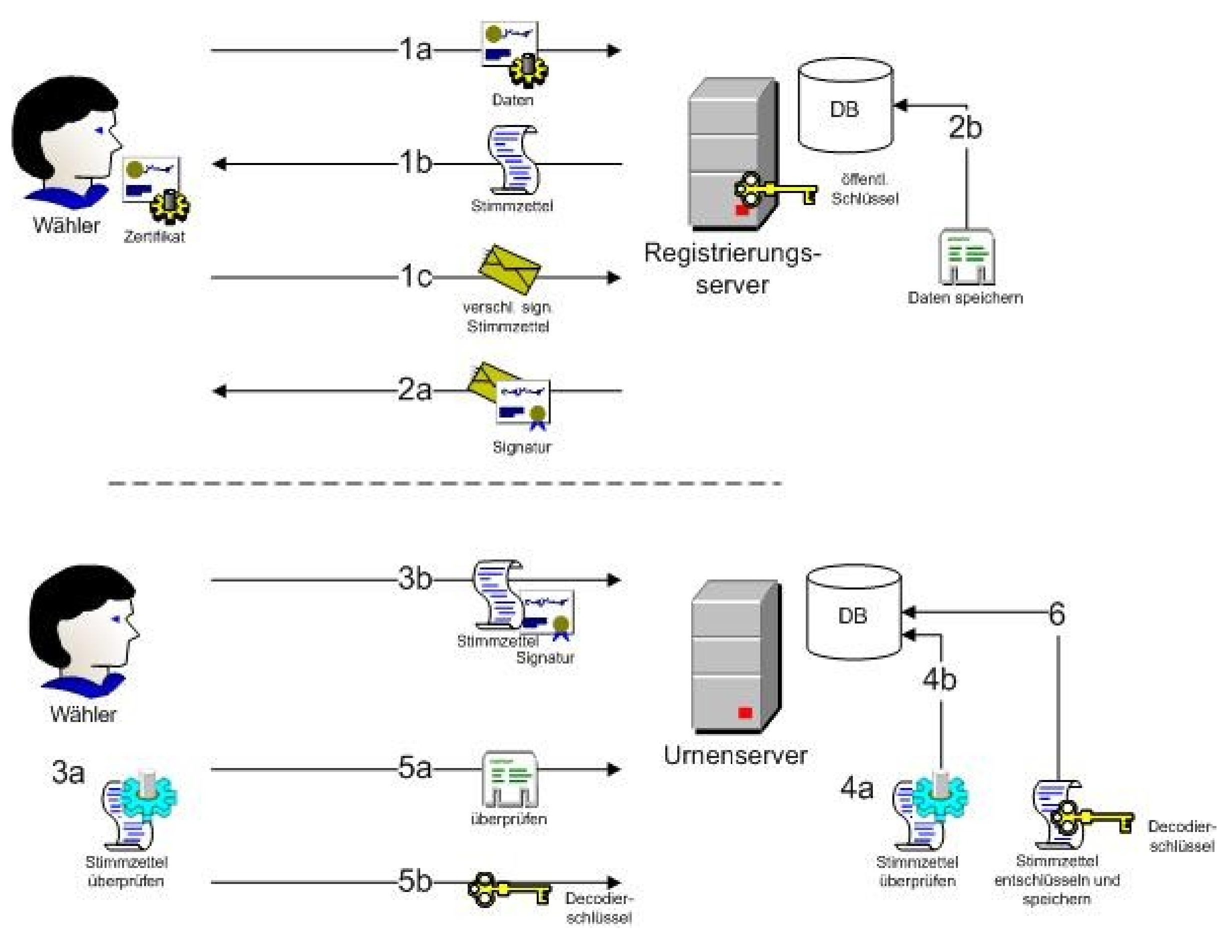


Abbildung 14: Schritte des Wahlverfahrens nach Fujioka et al [FuOk93]

- *S*chritt 1 (*Preparation*): Der Wähler erhält über anonyme Kanäle seinen digitalen Stimmzettel und trifft seine Entscheidung. Der ausgefüllte Stimmzettel *SZ* wird mit einem Schlüssel *m* ver-

schlüsselt und der Wähler erhält *m(SZ)*. Dann wird der Stimmzettel auf die Blinde Signatur vorbereitet (blindisiert) - das Ergebnis ist ein blind verschlüsselter Stimmzettel *b(m(SZ))*. Die Nachricht wird mit dem privaten Schlüssel *v* (des asymmetrischen Schlüsselpaares, bestehend aus einem öffentlichen und einem privaten Schlüssel) des Benutzers signiert *[b(m(SZ))]v* und an den Registrierungsserver geschickt.

- Schritt 2 (*Administration*): Der Server überprüft, ob der Wähler das Recht hat abzustimmen, ob er bereits eine Signatur angefordert hat und ob die Signatur des Wählers stimmt (Überprüfung mit dem öffentlichen Schlüssel des Wählers). Nach der Überprüfung unterschreibt der Registrierungsserver die für ihn nicht zu entziffernde Nachricht mit seinem privaten Schlüssel *d* und schickt das Paket *[b(m(SZ))]d* wieder zurück zum Wähler. Zusätzlich wird eine Liste geführt, wessen Stimmzettel bereits signiert wurde.
- Schritt 3 (*Voting*): Der Wähler überprüft die Signatur des Registrierungsservers mit dessen öffentlichen Schlüssel, entfernt die Verschlüsselung, die sogenannte Blindisierung, und erhält den verschlüsselten und authentisierten, da signierten, Stimmzettel *[m(SZ)]d*. Dieser Stimmzettel wird nun an den Urnenserver geschickt.
- Schritt 4 (*Collecting*): Wurde der verschlüsselte und signierte Stimmzettel erfolgreich empfangen, wird die Signatur des Registrierungsservers mit dessen öffentlichen Schlüssel überprüft und der Stimmzettel noch verschlüsselt in einer Liste gespeichert.
- Schritt 5 (*Opening*): Der Wähler überprüft, ob sein Stimmzettel in der Liste der Stimmzettel enthalten ist, und schickt den Decodierschlüssel *m'* nachträglich an den Urnenserver.
- Schritt 6 (*Counting*): Mit dem Decodierschlüssel *m'* wird der Stimmzettel *m(SZ)* in der Urne entschlüsselt, der Stimmzettel *SZ* wird überprüft und die Stimme zu den Resultaten gespeichert.

Bekannte E-Voting-Systeme basierend auf diesem Wahlprotokoll sind z. B. Lorrie Cranor's Sensus Protokoll [CrCy97], REVS von Joaquim et al [JoZu03] oder Votescript [OlGa06], wie auch eine Erweiterung des Wahlschemas der Autoren selbst [OhMi99].

Der Nachteil dieser Methode ist die Komplexität, die Implementierungsfehler nicht ausschließen lässt. Dieses Verfahren setzt weiters einen sicheren anonymen Übertragungskanal voraus, ohne ihn aber genauer zu spezifizieren.

4.4.1.2 Andere Verfahren basierend auf Blinden Signaturen

Weitere Verfahren, die auf Blinden Signaturen basieren, sind etwa das von Okamoto [Okam97], eines von Sako [Sako94] oder das von Baraani [BaPi94] und andere [BaFa04, Dini02, Dini02a, Ga-

Ro05, HoMi95, JaCh01, JuLe02, JuLe97, KiSa03, Okam96, RaRa01, YuLe03, YuLe04]. Das mobile E-Voting-System, oder auch M-Voting-System, von Barbara Ondrisek [OnGr05] erweitert das Verfahren nach Fujioka et al ebenfalls.

Einige E-Voting-Systeme adaptieren das Verfahren und verwenden mehrere Server (Administrator-, Registrierungs-, Validierungs- und Urnenserver) zur Aufteilung der Zuständigkeiten, wie das von Ibrahim et al [IbKa03], oder permutierte Kandidatenlisten (siehe Kapitel 4.4.2).

Viele E-Voting-Systeme bedienen sich Smartcards[41] zur Identifizierung und Authentifizierung der Wähler und / oder der Wahladministration und zur Verschlüsselung der Stimmzettel. Die Smartcard nimmt somit oft eine wichtige Rolle im E-Voting-Prozess ein [WaCo02].

4.4.2 Permutierte Kandidatenlisten

Einige Weiterentwicklungen von E-Voting-Systemen verwenden einen Scrambling-Algorithmus, der eine Permutation[42] der Reihenfolge der Kandidaten ausgibt. Ein Stimmzettel wird mit einer in ihrer Reihenfolge veränderten Kandidatenliste dargestellt, und eine Stimme wird gemäß dieser veränderten Reihenfolge (somit verschlüsselt) abgegeben. Die abgegebene Stimme wird erst nach der Sammlung der Stimmzettel entschlüsselt, indem die Stimme entsprechend der Permutation wieder korrekt zugeordnet wird.

Eine Papierstimmzettel-Variante eines E-Voting-Systems mit Scrambling-Algorithmus wurde mit *Scratch & Vote* von Ronald L. Rivest entwickelt. Die Parteien werden in jeweils unterschiedlicher Reihenfolge auf dem Stimmzettel dargestellt, und die Folge der Permutation wird zu jedem Stimmzettel in einem zweidimensionalen Barcode gespeichert. Der Stimmzettel besteht weiters aus zwei Teilen: zum einen aus der Liste der Kandidaten und zum anderen aus der zugehörigen Liste der Felder für die Markierungen (Kreuze).

Der Wähler gibt seine Stimme durch Ankreuzen der Kästchen oder ähnlich ab und entfernt die eine Hälfte des Stimmzettels, auf der die Auflistung der Kandidaten dargestellt wird. Nur die zweite Hälfte, die nur noch die Markierungen der abgegebenen Stimmen enthält, wird somit verschlüsselt (da die Reihenfolge nicht erkennbar ist) abgegeben. Mit dem Barcode, der sich auf dem Abschnitt befindet, kann die Verschlüsselung der Reihenfolge decodiert werden und die Stimme den Kandidaten zugeordnet werden (siehe Abbildung 15).

[41] Smartcards sind Plastikkarten mit einem eingebetteten Mikroprozessor und Speicher [Hass01, S. 75].

[42] Eine Permutation ist eine Veränderung der Reihenfolge einer Menge durch Vertauschen ihrer Elemente.

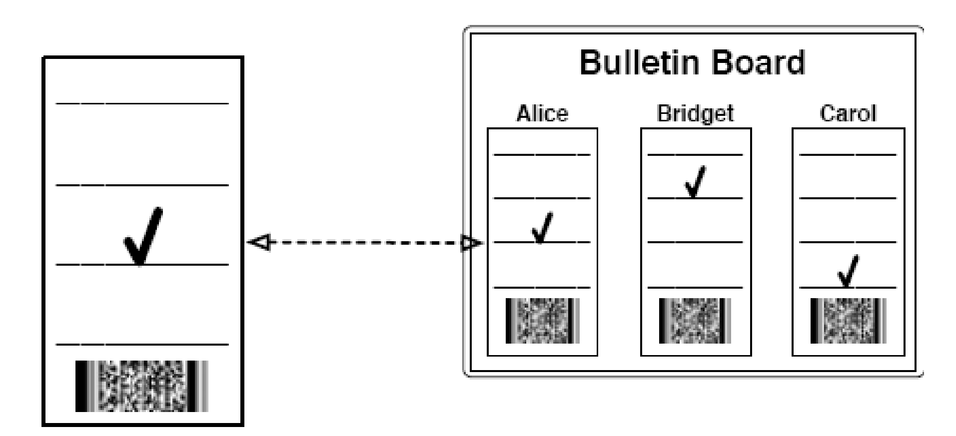


Abbildung 15: Verifikation der Scratch & Vote Methode, Quelle [AdRi06]

Weiters kann der Wähler seine abgegebene Stimme mit dem Beleg über ein Interface im Internet (auf einem *Bulletin Board*, siehe Kapitel 6.7.2) überprüfen, ob der Barcode zur gespeicherten Stimme auch mit dem Barcode auf dem Beleg übereinstimmt, und wird somit Teil eines Audit-Prozesses [AdRi06].

Dieser Ansatz ist eine Variante des *Prêt à Voter* Schemas [ChRy05] von Peter Ryan von der Universität of Newcastle, das ursprünglich ohne Papierstimmzettel entwickelt wurde, aber später um on-demand Stimmzettelausdrucke und erneute Verschlüsselungsmischungen erweitert wurde [RySc06]. Diese beiden Systeme werden auch *End-to-End Systeme* genannt, da sie die Verifizierung der abgegebenen Stimme durch den Wähler ermöglichen (siehe Kapitel 6.7.2).

In einem theoretischen Ansatz namens *Vote Scrambling Algorithmus* wurde eine ähnliche Methode zur Permutierung der Kandidatenlisten vorgestellt, bei der eine Zufallszahl (One-Time-Pad Sicherheit[43]) die Reihenfolge der Kandidaten permutiert und die Stimme am Urnenserver entschlüsselt wird [FiZu05].

4.4.3 Verdeckte Auswertung

Bei E-Voting-Systemen mit verdeckter Auswertung wird die Stimme mit Zuordnung zum Wähler verschlüsselt an den Urnenserver geschickt, der mit einem speziellen mathematischen Verfahren eine verschlüsselte Summe der Stimmen bildet. Alle Stimmen bilden zusammen ein einziges großes Endergebnis, das nach Sammlung der Stimmen entschlüsselt wird. Die geheime Wahl wird trotz Zuordnung zu einer Person sichergestellt, da die Auswertung der Stimmen verdeckt erfolgt.

Dieser Ablauf wird in der Praxis durch zwei verschiedene Verfahren realisiert: Hardware Security Modules (HSM) oder homomorphe Kryptografie.

[43] One-Time-Pad werden symmetrische Einmalschlüsselverfahren genannt, bei denen ein zufällig erzeugter Schlüssel verwendet wird, der so lang ist, wie die Nachricht selbst.

4.4.3.1 Hardware Security Modules

Ein *Hardware Security Module* ist ein externes Gerät, das an eine Wahlmaschine angeschlossen wird. Das Modul generiert oder speichert Daten sicher.

> „HSM werden zur Wahrung der Anonymität in der Weise eingesetzt, dass die verschlüsselten Stimmen im HSM decodiert und ausgezählt werden, aber nicht einzeln, sondern nur in ihrer Summe ausgelesen werden können.“ [VoKr06, S. 106]

Ein HSM-System wurde bei Lokalwahlen im Herbst 2005 in Estland eingesetzt.

4.4.3.2 Homomorphe Kryptografie

Eine kryptografische Funktion *E* (basierend auf öffentlichen Schlüsseln) gilt dann als *homomorph*, wenn Folgendes für einen öffentlichen Schlüssel *K* gilt:

$$E_K(T_1 \oplus T_2) = E_K(T_1) \otimes E_K(T_2)$$

Das Funktionspaar $(\oplus,\otimes)$ kann jedes beliebige Paar (f_1,f_2) bilden, solange die Funktionen homomorphe Eigenschaften haben [RosI04, S. 26].

Es wird zwischen additiven (etwa in [Pail99, ElGa85]) und multiplikativen homomorphen Kryptosystemen (etwa in [RiSh78, PeAd04]) unterschieden.

Zur Wahlauswertung werden die verschlüsselten Stimmen miteinander multipliziert (oder addiert), das Produkt (oder die Summe) entspricht dem verschlüsselten Wahlergebnis $T_1 \otimes ... \otimes T_n$. Durch diese homomorphe Eigenschaft können Stimmen anonym gezählt werden, ohne eine einzelne Stimme zu entschlüsseln. Ein Beispiel für ein homomorphes Kryptosystem ist der multiplikativ homomorphe RSA Kryptografie-Algorithmus [RiSh78]. Bei diesem Verfahren werden keine Einzelstimmen gespeichert. Ein Nachteil dieser Methode ist die große Anzahl an Rechenoperationen, die diese Methode sehr langsam machen.

Eines der ersten Wahlprotokolle, in denen homomorphe Kryptografie verwendet wurde, war das von Cohen und Fischer [CoFi85]. Auf dem selben Ansatz basierend wurde eine Reihe weiterer Protokolle entwickelt [Acqu04, Bena87, BeYu86, CrFr95, CrGe97, DaJu03, GoZh02, Iver92, KiYu02, LeBo04, LeKi00, LeKi03, SaKi94, Okam96]. Eines der bekanntesten Protokolle, das homomorphe Kryptografie verwendet, wurde von Schoenmakers in seinem *Publicly Verifiable Secret Sharing* (PVSS) Scheme [Scho99] vorgestellt. Dieses basiert auf einem früheren Protokoll von Schoenmakers [CrGe97] und setzt neben homomorpher Kryptografie auch auf *Secret Sharing* [Sham79] (zu

Deutsch: „geheimes (Ver-)Teilen sensibler Daten“) und war Grundlage des EU Projekts CyberVote (siehe auch Kapitel 4.3.3).

Weiters verwendet das kommerzielle DRE-System *VoteHere* [AdDa00] ebenfalls homomorphe Verschlüsselung, neben weiteren Verfahren wie dem von Hirt [HiSa00], Damgård [DaJu01] oder Baudron [BaFo01].

4.4.4 Mehrstufige Verfahren

Mehrstufige Verfahren trennen den Prozess der Identifikation und Ausgabe der Stimmzettel von der Abgabe dieser. Die anonymen leeren Stimmzettel werden dabei meist auf einem Trägermedium wie einer Smartcard gespeichert.

Das Verfahren von Bruck et al [BrJe01] unterteilt das Wahlprotokoll in folgende Schritte, wobei eine Metapher für den Stimmzettel (der Frosch / The Frog), der sich auf einem Speichermodul befindet, verwendet wird:

- Initialisierung (*Signing in*)
- Treffen einer Wahl (*Vote generation*)
- Stimmabgabe (*Vote casting*)

Mit dieser „modularen Wahl-Architektur“ wird die Stimmgenerierung von der Stimmabgabe getrennt.

Das Wahlverfahren nach Prosser / Müller ist ebenfalls ein mehrstufiges Verfahren. Zur Gewährleistung der Anonymität wird der Wahlvorgang in zwei zeitlich getrennten Phasen abgehalten: Im ersten Schritt, der Registrierung, werden elektronische, anonyme Stimmzettel auf mobile Trägermedien verteilt, die dann in der zweiten Phase abgegeben werden können [PrMu02].

Ein Problem bei diesem Verfahren ist die Zwischenspeicherung des Stimmzettels auf einem Datenträger, wie einer Smartcard, einer Signaturkarte oder einem anderen Medium, da durch ein mögliches Auslesen und Manipulieren der Daten die Wahlrechtsgrundsätze der geheimen und gleichen Wahl gefährdet werden könnten.

4.4.5 Wahlprotokolle basierend auf Mix-Nets

Diese Wahlschemata basieren auf sicheren, anonymen Kanälen und digitalen Pseudonymen. Verfahren mit Mix Networks wurden das erste Mal von David Chaum vorgestellt [Chau81], wobei Daten über ständig wechselnde Routen über mehrere Nodes geschickt werden, und wurde seitdem auch weiterentwickelt und erweitert [BoGo02, Boyd90, Chau88, Jako98, JuCa02, LeBo04, Neff04].

Im Allgemeinen wird zwischen *Decryption Mixnets* und *Re-Encryption Mixnets* unterschieden, wobei letztere Mix Networks als fehlerrobuster gelten [SaPo06].

Weitere E-Voting-Verfahren basierend auf Mix-Nets sind die von Park et al [PaIt93], von Sako [SaKi95, OgKu97] und von Masayuki Abe [Abe99].

4.4.6 Andere Wahlprotokolle und Probleme

Einige jüngere E-Voting-Verfahren, wie von Chaum [Chau04], Rivest [Rive06] oder Ryan [ChRy05], erweitern herkömmliche Verfahren um *Bulletin Boards*, mit deren Hilfe eine Stimme nach der Stimmabgabe anonym überprüft werden kann (siehe Kapitel 6.7.2).

In dem Wahlschema von Kiayias und Yung wird eine Kombination aus Mix-Nets (siehe Kapitel 4.4.5) und homomorpher Kryptografie (siehe Kapitel 4.4.3.2) vorgestellt [KiYu04].

Das Internet-Wahlverfahren von Karro und Wang verwendet weder Blinde Signaturen, noch anonyme Kanäle, sondern basiert auf *Trusted Authorities* und läuft in vier Phasen über verschiedene, getrennte Server ab [KaWa99]. Ein anderes E-Voting-Protokoll verwendet keine Kryptografie, sondern „schwache Signaturen" und Vektoren, um Sicherheit zu gewährleisten [MaMa07].

Das Verfahren nach Chen und Horng ist für kleinere Online-Wahlen gedacht und basiert auf *Private Infomation Retrieval* [ChGo95] mit nur einem Server mit einem *Secure Coprocessor* [ChHo05].

Auf einer ganz anderen Technologie setzen Park und Shin auf, die einen *Intelligent Magic Sticker* verwenden. Dieser ist ein holografischer Aufkleber, der, je nachdem aus welchem Winkel man ihn betrachtet, verschiedene Informationen erkennen lässt. Diese Informationen werden zum Anonymisieren der Stimme des Wählers verwendet [PaSh06].

Die theoretischen Ansätze zu Wahlverfahren sind sehr fundiert. Analysen von E-Voting-Schemata [GoKl06] haben aber erwiesen, dass auch die theoretische Basis eines elektronischen Wahlverfahrens - sprich das Wahlprotokoll selbst - oft fehleranfällig sein kann. Vergleichende Arbeiten [SaPo06, Grit03] über die Sicherheit elektronischer Wahlverfahren haben auch gezeigt, dass man bei der Auswahl eines E-Voting-Protokolls Kompromisse eingehen muss, da nicht alle Facetten von Sicherheit durch ein Protokoll abgedeckt werden.

Weiters sind durch die Komplexität der Protokolle Implementierungsfehler nicht auszuschließen. Oft muss auch zwischen Sicherheit und Usability bei der Implementierung abgewogen werden [DaGr03].

4.5 E-Voting in Österreich

Bei der Einführung von E-Voting in Österreich müssen die Richtlinien und Verordnungen des Wahlrechts (siehe Kapitel 2), des E-Government Gesetzes [BGBl04] und des Signaturgesetzes

[BGBl99a] eingehalten werden. Im E-Government Gesetz wird das Konzept Bürgerkarte[44] vorgestellt, das Personenanbindung, elektronische Signaturen und Zertifikate inkludiert [Holz05].

Weiters gibt es eine Empfehlung des Europarats für E-Voting-unterstützte Wahlen [CoE04] (siehe auch Kapitel 6.8.4), womit die E-Voting-Initiative in Österreich bestärkt wird. Eine Empfehlung des Europarates sieht allerdings vor, elektronische Wahlen parallel zum konventionellen Stimmabgabeverfahren zu betreiben. Hier muss auf das Risiko von Mehrfachabstimmungen geachtet werden, da die Wählerevidenzen synchron gehalten werden müssen.

4.5.1 Pilotversuche

Mitarbeiter der Wirtschaftsuniversität Wien (vor allem Robert Krimmer und Alexander Prosser) haben bereits zwei Pilotversuche zu E-Voting durchgeführt, bei denen die technische Realisierbarkeit evaluiert wurde. Diese Versuche wurden parallel zu den Österreichischen Hochschülerschaftswahlen 2003 [PrKo02] und zur Wahl des österreichischen Bundespräsidenten 2004 durchgeführt [StWe05, PrKo04].

Beim Pilotversuch an der Wirtschaftsuniversität Wien parallel zu den Österreichischen Hochschülerschaftswahlen war eine Internetwahl möglich, an der rund 1.000 Studenten teilnahmen. Die Studenten mussten sich vor der Stimmabgabe registrieren und erhielten einen elektronischen Stimmzettel, der auf einem Speichermedium zwischengespeichert wurde (siehe auch Kapitel 4.4.4).

Bei dem Wahltest parallel zu den Bundespräsidentschaftswahlen haben 1.786 von rund 20.000 WU-Studenten einen elektronischen Stimmzettel beantragt, 961 haben ihre Stimme tatsächlich auch über das E-Voting-System abgegeben. Dabei wurde ein sehr ähnliches Wahlergebnis (Abweichung von 0,6 %) zu den offiziellen Wahlresultaten der Wahl erzielt. Der Ablauf war sehr ähnlich zum vorangegangenen Pilotversuch: Die Studenten identifizierten und registrierten sich über das Internet vor der Wahl, die Stimmabgabe mit einem anonymen elektronischen Stimmzettel erfolgte ebenfalls über das Internet.

Die *Wiener Zeitung* hat 2006 mit Unterstützung der WU Wien (vor allem durch Alexander Prosser) ebenfalls eine elektronische Testwahl via Internet für 300 Auslandsösterreicher mit breiter Zustimmung durchgeführt. Die Teilnehmer wurden befragt, welche Neuerungen bei Wahlen sie sich wünschten und 79,7 % der Befragten gaben eine eine Wahlmöglichkeit über das Internet zusätzlich

[44] Die Bürgerkarte leidet an mangelnder Verbreitung. Das scheint am hohen Zusatzaufwand zu liegen, denn neben der Chipkarte selbst ist eine spezielle Software und ein Kartenlesegerät notwendig, um sich dieser Technologie zu bedienen. Der damit verbundene finanzielle Aufwand beläuft sich auf einmalig ca. 70 € (Registrierungs- und Kartengebühr und Kartenlesegerät) und jährlich ca. 20 € [Reis05]. Durch die künftige Einbindung der Bürgerkartenfunktionalität in die e-Card sollen diese Kosten allerdings reduziert werden.

zu herkömmlichen Verfahren an. Der Prototyp wurde zudem durch den Sicherheitsexperten Herbert Leitold (A-SIT[45]) untersucht, der einige Sicherheitslücken fand. [PrSt06]

Das Wirtschaftskammergesetz [WKG98, § 74 Abs 2-4] erlaubt wie das Hochschülerinnen- und Hochschülerschaftsgesetz [HSG98, § 34 Abs 4-7] bereits seit 2001 elektronische Wahlen unter Verwendung elektronischer Signaturkarten. Bei den Wirtschaftskammerwahlen 2000 wurden die 64 Wahllokale in Wien miteinander vernetzt und an eine zentrale Wählerevidenz angebunden [Krim03].

4.5.2 Arbeitsgruppen

Im Frühjahr 2004 wurde vom Bundesministerium für Inneres eine Arbeitsgruppe gebildet, die sich „mit der Sichtung von E-Voting-Projekten im In- und Ausland, der Prüfung der Umsetzbarkeit der Empfehlung des Ministerkomitees des Europarates zu E-Voting und mit rechtlichen, technischen und ökonomischen Erfordernissen im Falle der Umsetzung eines E-Voting-Konzepts in Österreich auseinandergesetzt“ [BMI04] hat.

Der Abschlussbericht der Arbeitsgruppe und ihrer Untergruppen [BMI04] zeigte auf, dass eine Änderung des Wahlrechts vorgenommen werden müsste, zusammen mit einer erneuten Definition des geheimen und persönlichen Wahlrechts, um E-Voting in Österreich einführen zu können. Die Wahlgrundsätze (siehe auch Kapitel 2.1) müssen ebenfalls auf technischer Ebene sichergestellt werden, hohe Technik-, Qualitäts- und Sicherheitsstandards müssen eingehalten werden etc.

Der Bericht sieht aus finanziellen und logistischen Gründen E-Voting-Maschinen in Wahllokalen nicht in Betracht, sondern schlägt Internetwahlen vor.

Allerdings sprach sich der Abschlussbericht für E-Voting nur als Alternative zu traditionellen Wahlen aus, die herkömmlichen Wahlen könnten durch eine E-Voting-Variante ergänzt, aber nicht ersetzt werden. Von einem derartigen Vorhaben - Papierstimmzettel und elektronische Stimmzettel parallel als Wahlmedium anzubieten - wird jedoch weitgehend abgeraten [XeMa04].

4.5.3 Zukunft des E-Votings in Österreich

Bei der EU-Wahl 2009 und bei den ÖH-Wahlen 2009 (siehe auch Kapitel 4.5.1) sollen bereits rechtsgültige Internetwahlen in Österreich eingeführt werden - so das politische Ziel der Parteien. Eine Bestrebung Wahlmaschinen in naher Zukunft einzusetzen gibt es derzeit nicht. Der Fokus liegt vorrangig auf Internetwahlsystemen, um Auslandsösterreichern eine alternative Form der Stimmabgabe zu ermöglichen bzw. I-Voting für Vereinswahlen einzusetzen. Eine Liste der österreichischen E-Voting-Initiativen wird im Anhang gegeben (siehe Appendix B).

[45] A-SIT: Zentrum für sichere Informationstechnologie - Austria.

Wissenschaftsminister Johannes Hahn fordert ebenfalls E-Voting für die ÖH-Wahl 2009 zuzulassen, allerdings meldet die Österreichische Hochschülerschaft (ÖH) Bedenken an, als „E-Voting-Versuchskaninchen“ (siehe Kapitel 4.5.1) bereit zu stehen. Der Verfassungsrechtler Heinz Mayer bezweifelt die Verfassungskonformität der elektronischen Stimmabgabe und zweifelt an E-Voting, wie auch der Präsident des Verfassungsgerichtshofes (VfGH) Karl Korinek.

Das Hochschülerinnen- und Hochschülerschaftsgesetzes ermöglicht bereits seit 2001 die elektronische Stimmabgabe [HSG98, § 34 Abs 4-7] mit digitalen Signaturkarten. Hahn besteht auf den Einsatz von E-Voting bei den kommenden ÖH-Wahlen, notfalls auch gegen den Willen der ÖH.

Die Einführung von E-Voting in Österreich ist mit dem Beschluss des Regierungsprogramms für die XXIII. Gesetzgebungsperiode [BKA07, S. 28] und dem Wahlrechtsreformpaket des Ministerrates - wenn es nach bestimmten Politikern gehen soll - nur noch eine Frage der Zeit, da erstens die Stimmabgabe im Inland mittels Briefwahl (mit Wahlkarten, bisher nur aus dem Ausland möglich) vorgesehen ist und somit das Briefwahlrecht als Grundlage für E-Voting gelockert wird (vgl. Kapitel 2.3), und zweitens bereits eine weitere Prüfung (dieses Mal durch Vizekanzler Molterer) der elektronischen Stimmabgabe geplant ist.

Für eine Einführung der Wahlen auf nationaler Ebene ist allerdings eine Änderung des Bundes-Verfassungsgesetzes notwendig, da das derzeitige Recht eine persönliche Stimmabgabe im Wahllokal in der Wahlzelle mittels eines amtlichen (Papier-)Stimmzettels vorsieht [BGBl92 § 57]. Eine Verfassungsänderung kann aber nur relativ schwer veranlasst werden, da dafür eine 2/3 Mehrheit im Parlament notwendig ist.

5 Sicherheitsrisiken von E-Voting-Systemen

Die Sicherheitsrisiken elektronischer Wahlsysteme sind vielfältig. In diesem Kapitel wird ein Überblick über mögliche Attacken, Risiken und Betrugsarten, sowie zahlreiche Beispiele zu Fehlern, Schwachstellen und Pannen gegeben.

5.1 Physikalische, syntaktische und semantische Attacken

Es kann zwischen physikalischen Attacken, syntaktischen Attacken und semantischen Attacken unterschieden werden (vgl. physische Sicherheit, technische Sicherheit und organisatorische Sicherheit in Kapitel 3.5) [Schn00].

Physikalische Attacken richten sich gegen die benutzte Hardware und die Netzverbindung zwischen den einzelnen Einheiten (siehe Kapitel 5.4.1). *Syntaktische Attacken* hingegen gefährden die eingesetzte Software, die verwendeten Algorithmen, Regeln, Prozeduren und Abläufe (siehe Kapitel 5.4.2).

Weiters gefährden *semantische Attacken* die Zuweisung einer bestimmten Bedeutung zu einem Inhalt, wobei damit gemeint ist, dass Fakten oft als das genommen werden, als was sie dargestellt werden und selten hinterfragt werden. Bei semantischen Attacken wird elektronische Information so manipuliert, dass das Resultat korrekt aussieht, obwohl es falsch ist.

> „Semantic attacks directly target the human/computer interface, the most insecure interface on the Internet. Amateurs tend to attack machines, whereas professionals target people. Any solutions will have to target the people problem, not the math problem." [Schn00, S. 168]

Im Bezug auf elektronische Wahlen könnte das bedeuten, dass der Wähler manipuliert wird und denkt, er stimmt für Kandidat A, in Wirklichkeit seine Stimme aber für Kandidat B abgibt. Ein Beispiel hierfür ist die Kalibrierung von Touchscreen-Monitoren (siehe auch Kapitel 5.4.3).

5.2 Retail Fraud und Wholesale Fraud

Weiters gibt es eine Unterscheidung zwischen *Retail Fraud* und *Wholesale Fraud* [Rubi06, S. 37]. Bei einem Retail Fraud müsste ein Angreifer jede Maschine einzeln angreifen. Das ist bei eher traditionelleren E-Voting-Verfahren wie Hebelmaschinen (Lever Voting Machines) oder optischen Scannern (Optical Mark-Sense Wahlsysteme) der Fall. Der Angreifer bräuchte physischen Zugriff auf die

einzelnen Maschinen und hätte großen Aufwand, alle Maschinen zu manipulieren, ohne entdeckt zu werden.

Im Gegensatz dazu könnte bei einem Wholesale Fraud das gesamte System mit vielen Maschinen an verschiedenen Orten von einem einzelnen Punkt aus angegriffen werden. Auf diese Art kann mit kleinem Aufwand (bzw. mit trivial kleinem Aufwand [DiPe04]) großer Schaden entstehen. Das ist bei Wahlmaschinen ohne Papierstimmzettel der Fall.

5.3 Risiken bei Urnenwahlen

Wenn man Sicherheitsrisiken elektronischer Wahlen betrachtet, dürfen die Risiken herkömmlicher Wahlen mit Urnen (siehe auch Kapitel 2.2) nicht außer acht gelassen werden. Die Bedrohungen, die bei gängigen Wahlen herrschen, gelten auch bei E-Voting-Systemen. Ein wichtiges Entscheidungskriterium für den Einsatz elektronischer Wahlen ist daher, dass sie mindestens so sicher sein müssen wie die bisher eingesetzten Wahlformen.

Potenzielle Angriffsziele sind die Wähler, die Beisitzer[46] der örtlichen Wahlbehörde, die Urne, der Übertragungskanal für das Endergebnis oder die zentrale Wahlkommission [Schn04, S. 280ff].

Bestechungen von *Wählern* sind ein traditionelles, aber immer noch aktuelles Problem. Erst 1996 wurden 21 Personen in Dodge County, Georgia, USA, wegen ungesetzlicher Wahlpraktiken verurteilt. Wahlkabinen können Stimmenkauf zwar einschränken, jedoch wird diese Form der Wahlmanipulation mit neuen Technologien, wie etwa mit Handykameras mit Foto-Funktion, wieder zu einem Thema. Distanzwahlen wie die Briefwahl (oder Internetwahlen) sind in diesem Bereich besonders problematisch (siehe auch Kapitel 1.4).

Die Anonymität der Wähler ist ebenfalls gefährdet, wenn man Papierstimmzettel auf Spuren des Wählers, etwa DNS oder Fingerabdrücke, untersuchen würde. Selbes gilt für versteckte Kameras in Wahlkabinen.

Korruption der *Beisitzer*, die für Identitätsprüfungen, Autorisierungen und Zählungen zuständig sind, kann derart genutzt werden, dass manche Personen mehrfach wählen können oder Wähler in die Wählerevidenz gesetzt werden, die nicht wahlberechtigt sind (zu junge, verstorbene oder erfundene Personen). Bei der Auszählung der Stimmen kommt es oft zu Unstimmigkeiten der Ergebnisse, nicht zuletzt durch den Interpretationsspielraum der Personen, die die Stimmen auswerten. Erneute Auszählungen der Papierstimmzettel schwächen dieses Problem allerdings ab.

Wahlurnen könnten mit bereits ausgefüllten Stimmzetteln gefüllt werden, allerdings wird eine derartige Manipulation durch eine Überprüfung der Übereinstimmung der Anzahl der Stimmzettel

[46] Beisitzer sind entweder Mitglieder der Sprengelwahlbehörde bestehend aus einem Vorsitzenden und drei Beisitzern [BGBl92, § 9] oder Mitglieder der Gemeindewahlbehörde bestehend aus einem Vorsitzenden und neun Beisitzern [BGBl92, § 8].

mit der der Wähler, die gewählt haben, verhindert. Ein Austausch einer gesamten Urne auf dem Weg vom Wahllokal zum Hinterzimmer, in dem ausgezählt wird, ist durch die Anwesenheit der Beisitzer schwierig.

Der *Übertragungskanal* für das Endergebnis per Telefon, Telefax, Bote oder Internet ist anfällig für Man-In-The-Middle[47] Attacken, allerdings gibt es in Österreich ein duales System. Eine für Attacken anfällige Sofortmeldung eines Zwischenergebnisses geht über ein Zwischenmedium zunächst an die Bundeswahlbehörde. Nach etwa 3 Wochen kommt es aber zu einer Niederschrift im Wahlakt, der schwerer gefälscht werden kann.[48]

Eine Bestechung der *zentralen Wahlkommissionen*[49] ist problematisch, da diese stark in der Öffentlichkeit stehen und zudem aus vielen Mitgliedern (zehn bis 18) bestehen, daher kann dieser Punkt vernachlässigt werden.

Letzten Endes hängt eine Urnenwahl stark von der Integrität der beteiligten Personen ab und damit auch vom Vertrauen in das System. Bei Urnenwahlen ist die Transparenz des Ablaufes gegeben und durch Wahlbeobachter und Beisitzer verschiedener Parteien gesichert. Diese Transparenz, somit auch das Vertrauen in den gesamten Prozess, ist bei elektronischen Wahlen schwer zu gewährleisten (siehe auch Kapitel 6.5).

5.4 Risiken von E-Voting-Systemen nach System-Komponenten

Im Folgenden wird eine kurze Übersicht über mögliche und beispielhafte Sicherheitsrisiken von E-Voting-Systemen gegeben. Geordnet werden die Risiken je nach System-Komponente (siehe Kapitel 4.2): Hardware, Software und Human Factors.

5.4.1 Hardware

Hardware-Sicherheitsrisiken betreffen mechanische, wie auch elektronische Komponenten. Beispiele für Sicherheitsrisiken, die die eingesetzten Computer, Speichermedien und Peripheriegeräte betreffen, werden folgend angeführt.

---

[47] Auch *Janusangriff* genannt. Der Angreifer fängt die Kommunikation zwischen zwei Teilnehmern ab und verändert diese.

[48] Quelle: Telefonat mit Mag. Robert Stein, Bundesministerium für Inneres, Sektion III - Recht, Abt. III/6 - Wahlangelegenheiten vom 17.4.2008.

[49] Zentrale Wahlbehörden sind die Bezirkswahlbehörden [BGBl92, § 10] und die Landeswahlbehörden [BGBl92, § 11], die jeweils aus 10 Mitgliedern bestehen, neben der Bundeswahlbehörde [BGBl92, § 12], die aus 18 Personen gebildet wird, darunter zwei Richter.

5.4.1.1 Mechanische Probleme

Mechanische Probleme beim Zählen von Lochkarten sind ein weit verbreitetes Problem. Bei sogenannten *Punch Card Systems* (Lochkartensystemen) gibt es Schwierigkeiten bei der Auswertung mittels optischer Scanner (Optical Mark-Sense Wahlsysteme). Wenn die Stimmfelder unvollständig ausgestanzt werden oder Stanzreste hängen bleiben (*Undervote*), sind die Wahlkarten nicht mehr korrekt lesbar. Selbes gilt, wenn der Wähler unabsichtlich zu viel weg gestanzt hat, dann spricht man von *Overvote*. Die nicht zu Ende geführte manuelle Neuauszählung in Florida 2000 ergab eine Fehlerrate von 5.68 % bei Auswertungen mittels optischer Scanner und 3.93 % bei Lochkarten [ArMo05]. Tabelle 5 zeigt die durchschnittlichen Fehlerraten der Wahlsysteme in den USA.

Systemtyp	*Durchschnittliche Fehlerrate*
Punchcard (Lochkarten-Systeme)	2.64
Papierstimmzettel	1.99
Lever machines (Hebelmaschinen)	1.72
DREs (Wahlcomputer)	1.68
Marksense (Optische Scanner)	1.37
U.S. Durchschnitt	*1.94*

Tabelle 5: Durchschnittliche Fehlerrate geordnet nach Wahlsystemen [BrBu01, S. 29]

Die geforderte erneute manuelle Auszählung der Lochkarten bei den Präsidentschaftswahlen 2000 in Florida wurde zwar begonnen, der Oberste Gerichtshof stoppte diese jedoch, bevor sie komplett durchgeführt werden konnte und der Kandidat George W. Bush gewann mit einem Vorsprung von nur 537 Stimmen die Wahl in Florida und somit auch die Präsidentschaft. Der aktuelle Gouverneur von Florida Charlie Crist setzte im Frühjahr 2007 die Verwendung gängiger Papier-Stimmzettel mit optischen Scannern für die Wahlen 2008 durch, um im Zweifelsfall eine manuelle Nachzählung zu vereinfachen und die Wahl transparenter zu gestalten.

5.4.1.2 Speichermedien

Eine Studie des *Election Science Institute* (ESI) in San Francisco über eine Stichprobe von 467 von insgesamt 5407 in Ohio eingesetzten Diebold Wahlmaschinen stellte fest, dass 24 Stück der eingesetzten Speichermedien keine Daten der Wahl enthielten. Weiters zeigten 72 % der Wahllokale eine Diskrepanz zwischen der elektronischen Aufzeichnung der Stimmen auf den Speicherkarten der Maschinen und den Papierbelegen. Auf 42 % dieser Wahlmaschinen, auf denen unterschiedliche Stimmen gefunden wurden, betrafen diese Diskrepanzen mindestens 25 Stimmen [ESI06].

5.4.1.3 Papierrollen

Das Gesetz des Staates Ohio (wie auch das des Staates New York) legt seit 2005[50] fest, dass jede Wahlmaschine einen Papierbeleg enthalten muss, auf dem jede abgegebene Stimme festgehalten wird. Die Studie zeigte allerdings, dass Wählerstimmen selbst dann falsch aufgezeichnet werden können, wenn die Wahlmaschinen mit Papier-Sicherungen arbeiten. Die Papierbelege wurden mit gewöhnlichen Druckern auf Papierrollen gedruckt, was profunde Risiken wie Papierstaus, leere Tintenpatronen oder falsch eingelegte Rollen mit sich brachte. 10 % der Prüfbelege wurden entweder vernichtet, fehlten, waren leer, unlesbar, zusammengeheftet oder auf eine andere Art kompromittiert [Song06].

Werden die Stimmen auf einer fortlaufenden Papierrolle gedruckt, so ist das Wahlgeheimnis gefährdet, da man, über die zeitliche Ankunft der Wähler im Wahllokal und eine chronologische Liste der Stimmzettel, die Stimmen bestimmten Wählern zuordnen kann.

5.4.1.4 Boot Loader

Der Bericht des finnischen Computer-Experten Harri Hursti[51] [Hurs06] zeigte nach der Untersuchung der Diebold Wahlmaschinen der Serie *Tsx* beim sogenannten *Hursti-Hack* mehrere gravierende Sicherheitsmängel auf. So wurde festgestellt, dass mit dem Boot Loader[52] der Maschine das Betriebssystem wie auch der Boot Loader selbst zurückgesetzt oder ein anderes Betriebssystem installiert werden konnte. Der Boot Loader konnte die Funktionen des danach geladenen Betriebssystems (in diesem Fall Windows CE) verändern.

Durch die schlechte Sicherung des Gehäuses (nicht versiegelte Schrauben konnten gelöst werden, Plomben zur Sicherung fehlten) wurde der Zugriff auf das Mainboard erleichtert. So konnte über PCMCIA[53] Steckplätze oder einen versteckten MMC/SD[54] Steckplatz zusätzliche bzw. bösartige Software oder zusätzliche Boot Loader Dateien eingeschleust werden. Weiters wurde ein Jumper auf dem Mainboard gefunden, mit dem zusätzliche Features der Software aktiviert oder deaktiviert werden konnten. Da keine kryptografischen Signaturen oder andere Sicherheitsmaßnahmen verwendet

---

[50] Der „Count Every Vote Act of 2005“ wurde am 17.02.2005 von der Republikanerin Stephanie Tubbs Jones eingebracht.

[51] Harri Hursti hat zusammen mit Bev Harris und anderen Sicherheitsexperten in der Dokumentation „Hacking Democracy“ (2006) mitgewirkt [Film1].

[52] Ein Boot Loader ist spezielle Software, die durch das BIOS eines Rechners von einem bootfähigen Medium geladen, anschließend ausgeführt wird und dann weitere Teile des Betriebssystems lädt.

[53] PCMCIA (Personal Computer Memory Card International Association) ist ein Standard, der eine Schnittstelle für PC Karten darstellt.

[54] MMC (MultiMediaCard) und SD (Secure Digital) Karten sind austauschbare Flash-Speicherkarten.

wurden, hätten die Maschinen und die Software mit diesen Möglichkeiten bereits lange vor den Wahlen verändert werden können, ohne dass eine Spur der Veränderung erkennbar gewesen wäre.

5.4.1.5 Bildschirm-Abstrahlungen

Ein weiteres Sicherheitsproblem, das sich nur schwer verhindern lässt, ist das Abstrahlen der Bildschirmröhren oder LCD-Monitore, das mittels *Van-Eck-Phreaking* bzw. *TEMPEST*[55]-Analyse abgefangen werden kann, um Benutzereingaben auszuspionieren. Mit diesen technischen Methoden kann das Wahlgeheimnis unterminiert werden.

Bei einem Versuch einer niederländischen Aktivistengruppe wurde ein Tempest-Hack auf Nedap-Maschinen erfolgreich durchgeführt. Dabei konnte festgestellt werden, welche Tasten bei den Geräten gedrückt oder welche Partei auf dem Display dargestellt wurden (wurden eine Partei mit Umlauten im Parteinamen dargestellt, änderte sich die Refresh-Frequenz des Displays), selbst von außerhalb des Gebäudes. [GoHe06]

Ein ähnlicher Versuch, den Bildschirminhalt auszulesen, wurde durch eine Gruppe von Informatikern der deutschen Uni Saarland versucht, wobei das dargestellte Bild auf dem Monitor durch Reflexionen auf Gegenständen mit gekrümmten Oberflächen wie Teekannen, Tassen oder selbst Augen abgelesen werden konnte [BaDu08].

5.4.1.6 Bit Flipping

Ein *flipping Bit* ist ein nicht vorhersagbarer, sehr seltener, spontaner Speicherfehler, bei dem sich ein einziges gespeichertes Bit verändert (von 0 auf 1 oder umgekehrt). In Belgien kam es im Mai 2003 durch ein geflipptes Bit zu einem Fehler von 4096 Stimmen im Gesamtergebnis, die einem Kandidaten zusätzlich hinzugefügt wurden [DePr07]. Der Fehler wurde entdeckt, da die Anzahl der dieser Kandidatin zugeordneten Stimmen das mögliche Maximum überschritt.

5.4.2 Software

Sicherheitsrisiken im Bereich Software betreffen das verwendete BIOS, Boot Loader, Betriebssystem, Treiber, Compiler, Programme, Datenbanken, im Programm verwendete Regeln, Prozeduren, Abläufe und bis hin zur Implementierung des Wahlprotokolles (siehe auch Kapitel 4.4).

Einige Beispiele, die Sicherheitsrisiken im Bereich der Software betreffen, werden hier gezeigt.

[55] Tempest: Temporary Emanation and Spurious Transmission.

5.4.2.1 Proprietäre Software

Es gibt drei führende Hauptthersteller von E-Voting-Maschinen in den USA: *Diebold Election Systems*, *Sequoia* und *Election Systems & Software* (ES&S). Jeder dieser Hersteller hält aus Konkurrenzgründen den eigenen Sourcecode so weit wie möglich geheim und limitiert somit den Zugriff unabhängiger Prüfstellen auf diesen [Ston03]. Die eingesetzte Software für elektronische Wahlmaschinen wie z. B. DRE-Wahlsysteme (Direct Recording Electronic Systems) ist somit meist proprietär. Die Überzeugung, dass die Geheimhaltung des Quellcodes eines Systems zu mehr Sicherheit führt, ist weitläufig als *Security by Obscurity* (oder auch *Security through Obscurity*) bekannt. Eines der Hauptargumente für Security by Obscurity ist, den Angreifern keine Möglichkeit zu geben, Betriebsgeheimnisse und Sicherheitslücken ausspionieren zu können.

Das gegenteilige Konzept zu Security by Obscurity ist als *Security by Transparency* bekannt (siehe Kapitel 6.5).

5.4.2.2 Mangelhafte Zertifizierungen

Wahlmaschinen werden in den USA von drei privaten unabhängigen Unternehmen (*Ciber*, *Wyle* und *SysTest*) nach den Richtlinien und Standards der *Federal Election Commission* (FEC) [FEC01] getestet und zertifiziert (siehe auch Kapitel 6.9.2), allerdings ohne staatliche Aufsicht oder Beteiligung. Der Zertifizierungstestprozess der proprietären Software ist geheim und meist unvollständig, auch die Ergebnisse der Tests sind geheim. Die in Wahlsystemen eingesetzte kommerzielle Standard-Software (Commercial Off-the-Shelf (COTS) Produkte, z. B. Microsoft Access) wird in keinem der Tests überprüft, da dies die Richtlinien der Wahlkommission der Vereinigten Staaten nicht fordern. Die Aussagekraft der Zertifizierung ist zudem fraglich, da die Zertifizierung der Hersteller der Maschinen selbst beauftragt wird (siehe auch Kapitel 6.9) [Simo04].

5.4.2.3 Sicherheitslücken in bestehenden E-Voting-Systemen

In einer Reihe von bereits eingesetzten E-Voting-Systemen wurden Fehler durch Analysen oder Studien gefunden (siehe auch Kapitel 6.3).

Im Fall von Diebold, dem bekanntesten Hersteller von Wahlmaschinen, kam es durch einen ungesicherten FTP-Server dazu, dass der eigentlich geheim gehaltene Sourcecode der DRE-Wahlmaschinen unbeabsichtigt herausgegeben wurde. Dieser Sourcecode wurde 2003 von einigen Sicherheitsexperten genauer analysiert, die Ergebnisse wurden im *Rubin Report* (bzw. auch *Hopkins Report* oder *Hopkins / Rice Report* genannt) veröffentlicht [KoSt04]. Weitere Berichte in anderen Artikeln oder Büchern (etwa [Keig04], von Bev Harris [Harr04, S. 138ff], Doug Jones [Jone03] und Avi Rubin [Rubi06]) und weitere offizielle Untersuchungen der Maschinen dieses Herstellers (z. B.

[SAIC03] und [RABA04]), bestätigten im Wesentlichen die gefundenen Sicherheitsprobleme des vorangegangenen Berichts.

Unter anderem wurden in diesem Report große Sicherheitslücken gefunden, die teilweise erst nach der Veröffentlichung des Berichts vom Hersteller ausgebessert wurden. Einige der verheerendsten Sicherheitslücken, die aufgedeckt wurden: Wähler konnten ohne Rückverfolgbarkeit mehrere Stimmen abgeben und normale Wähler konnten administrative Funktionen aufrufen. Insider wie Wahl-Helfer, Softwareentwickler und Portiers hatten noch größere Möglichkeiten als gewöhnliche Wähler, das System zu manipulieren. Weiters existierte keine angemessene Verschlüsselung zwischen dem zentralen Server und den Terminals, was Man-In-The-Middle-Attacken möglich gemacht hat. Der Report gezeigte unter anderem auch, dass „geschlossener“ Code viele Risiken birgt und Reviews (Design-)Fehler frühzeitig erkennbar machen (siehe auch Kapitel 5.4.2.1).

Eine weitere Studie [FeHa06] über die Wahlmaschinen AccuVote-TS der Firma Diebold zeigte ebenfalls große Sicherheitslücken. Die Hauptkritikpunkte waren:

- Bösartige Software könnte unauffindbar integriert werden und könnte etwa Stimmen einer Partei stehlen oder löschen.
- Jeder, der physikalischen Zugriff zu den Wahlmaschinen oder auch nur zu den Speicherkarten hat, kann bösartige Software installieren. Wahl-Mitarbeiter und auch Dritte haben oft nicht überwachten Zugriff auf die Maschinen.
- Wahlmaschinen sind anfällig für Wahlmaschinen-Viren, die sich etwa über Speicherkarten automatisch und unsichtbar von Maschine zu Maschine ortpflanzen können, während der Aktivitäten vor oder nach der Wahl.
- Viele der Fehler betreffen die Software oder die Hardware. Die Wahlprotokolle müssten auch angepasst werden, um die Sicherheit zu gewährleisten (siehe auch Kapitel 4.4.6).

Im Auftrag der kalifornischen *Secretary of State* und obersten Wahlleiterin Debra Bowen wurden mehrere Gutachten zu drei E-Voting-Systemen, die bei den Primary-Wahlen im Frühling 2008 eingesetzt werden sollen, im Rahmen einer grundlegenden Sicherheitsüberprüfung ("Top-to-Bottom Review") der Wahlmaschinen erstellt. Das Ziel der Untersuchung war, die Sicherheitsbedenken der Wähler zu zerstreuen und das Vertrauen in elektronische Wahlsysteme in Kalifornien für die kommenden Vorwahlen zu steigern.

Bowen hatte Matthew Bishop von der University of California Davis und David Wagner von der UC Berkeley beauftragt, E-Voting-Systeme der Hersteller Diebold, Hart Intercivic, ES&S und Sequoia zu untersuchen. Zu Hilfe kamen mehrere Sicherheitsexperten wie Ed Felten und der finnische IT-

Spezialist Harri Hursti. Bishop leitete zudem ein *Red Team*[56] für eine *Penetration Study*[57], das die Aufgabe hatte, gezielt Sicherheitslücken in den Systemen zu finden.

Das Gutachten zum E-Voting-Touchscreen-System *AccuVote-TSX* von Diebold [Bowe07] ergab, dass selbst ein Einzeltäter Möglichkeiten hat, die Maschinen etwa mit einem Virus zu manipulieren. Ein Virus könnte sich von einer Wahlmaschine oder Speicherkarte über das verwendete Wahlmanagement-System *GEMS* ausbreiten und viele weitere Maschinen kompromittieren. Der Wahlablauf könne durch gezielt herbeigeführte Maschinenabstürze sabotiert werden und trotz Papier-Backups könne der Ausgang knapper Wahlen beeinflusst werden. Das E-Voting-System habe grundlegende Entwurfsfehler und richte sich nicht nach dem etablierten Stand der IT-Sicherheitstechnik, warnten die Experten im Gutachten.

Das zweite Gutachten zu *Hart Intercivic* [Bowe07a] zeigte ähnliche Gefahren auf. Es gibt Sicherheitslücken, über die der Sourcecode verändert werden könne, und die für einen eingeschleusten Virus Möglichkeiten bieten, sich zu verbreiten. Das dritte Gutachten zum E-Voting-System von *Sequoia* [Bowe07b] fand gravierende Architektur-, Logik- und Programmierfehler in der Software und Sicherheitslücken, durch die Stimmen manipuliert werden könnten. Die Wahlmaschinen von *Election Systems & Software* (ES&S) hätten bei der Untersuchung ebenfalls einbezogen werden sollen, da aber die angeforderten Testgeräte nicht rechtzeitig zur Verfügung standen, konnten diese Wahlmaschinen nicht überprüft werden. Die Konsequenz war die Entziehung der Zulassung der Geräte für den Staat Kalifornien ohne erneute Auflagen für die darauf folgenden Wahlen 2008.

Als Folge der Gutachten über die Systeme von Diebold, Hart Intercivic und Sequoia wurden die geltenden Zulassungen im Staat für alle Systeme entzogen. Die Hersteller mussten ihre Wahlsysteme grundlegend überarbeiten, die dann nur unter strengen Auflagen bei den Wahlen 2008 eingesetzt werden durften.

Wahlbeobachtungen des *Chaos Computer Club* in Deutschland bei der Einführung von Nedap-Wahlcomputern für die Oberbürgermeisterwahl in Cottbus [CCC06] zeigten zahlreiche Angriffspunkte. Angriffspunkte für Außentäter sind:

- Die Sicherung der Wahlmaschinen nach der Lieferung war mangelhaft, da es keine oder nur unzulängliche Beaufsichtigung gab.
- Die auf dem Gehäuse angebrachten Siegel und Schlösser hätten leicht manipuliert werden können.

[56] Der Begriff „Red Team“ stammt aus dem militärischen Bereich und bedeutet im Allgemeinen, dass eine Gruppe von Experten ein unabhängiges Review durchführt.

[57] Bei einer *Penetration Study* wird auf mehreren Wegen versucht in ein System einzudringen bzw. ein System abstürzen zu lassen.

- Die Überprüfung der Software bei Inbetriebnahme war mangelhaft, etwa wurde nur darauf geachtet, ob das Display der Maschinen eine bestimmte Zahl anzeigt.

Angriffspunkte für Innentäter:

- Die Vorbereitung und Konfiguration wurde in einem nicht öffentlich zugänglichen Wahlbüro getätigt. Die Wahlvorstände hatten keine Möglichkeit zu überprüfen, ob die Software der vorgeschriebenen Version entspricht oder ob sie manipuliert worden ist.
- Experten der Physikalisch-Technischen Bundesanstalt überprüften die Software, allerdings sind deren Methoden nicht öffentlich zugänglich.
- Der Schutz der beiden Schlüssel, die zur Freischaltung der Wahlcomputer verwendet wurden, war mangelhaft.

Im Mai 2007 haben Mitglieder derselben Organisation wiederum ein Gutachten zu den *Nedap* Wahlmaschinen erstellt, wobei sie bei der Analyse der Geräte auf erhebliche Sicherheitsmängel gestoßen sind. So wurde gezeigt, dass die Software in einfacher Weise manipulier- und angreifbar ist, die Zulassungs- und Prüfverfahren des deutschen Bundesinnenministeriums und der Physikalisch-Technischen Bundesanstalt ungeeignet sind, Manipulationen aufzudecken, und die Annahmen des deutschen BMI und der PTB über mögliche Wahlfälscher unrealistisch sind (siehe auch Kapitel 6.9.1) [KuRi07].

5.4.2.4 Schwache Algorithmen

Ein Verfahren zur nachträglichen Veränderung der Reihenfolge der abgegebenen Stimmen wurde beim System von Diebold angewendet, allerdings wurde ein „schwacher" Algorithmus, der *Linear Congruential Generator* (LCG) von Bruce Schneier, verwendet. Dieser als gilt als nicht sicher, da die ursprüngliche Reihenfolge wieder hergestellt werden kann. Der Autor selber sagt zu dieser Methode:

> „Unfortunately, linear congruential generators cannot be used for cryptography; they are predictable" [Schn96, S. 369]

Bei der Analyse des Systems von Diebold wurde ebenfalls festgestellt, dass der veraltete DES Verschlüsselungsalgorithmus [Bish05, S. 228ff] verwendet wurde, der durch Bruteforce Attacken innerhalb kurzer Zeit geknackt werden kann [Gilm98], und nicht die verbesserten Versionen wie Triple-DES oder AES.

Verschiedene vergleichende Analysen von E-Voting [SaPo06, Grit03] zeigten, dass auch die Grundlage von E-Voting-Systemen - das Wahlprotokoll selbst - fehlerbehaftet sein kann. So wird bei der Auswahl eines Wahlprotokolls oft ein Kompromiss eingegangen, da meist nicht alle Aspekte von Sicherheit berücksichtigt werden (siehe auch Kapitel 4.4.6).

5.4.2.5 Dedicated Special Purpose Machine

Der Hersteller der Nedap Wahlmaschinen startete einen Aufruf zum Beweis für die Aussage, dass man mit Nedap Wahlmaschinen auch Schach spielen könne. Dies sollte nicht möglich sein, da Wahlmschinen sogenannte *Dedicated Special Purpose Machines*[58] sind [Groe06]. Dem Aufruf folgte eine Gemeinschaftsaktion der holländischen Initiative *Wij vertrouwen stemcomputers niet* und des Chaos Computer Clubs Berlin (CCC) [GoHe06]. Den Aktivisten gelang es, das Schachprogramm *Tom Kerrigans Simple Chess Program TSCP* auf der Wahlmaschine Nedap ES3B zum Laufen zu bringen (siehe Abbildung 16).



Abbildung 16: Umfunktionierte Nedap Wahlmaschine mit Schachprogramm. Quelle [GoHe06, S. 10]

Mit diesem Hack wurde bewiesen, dass das Wahlergebnis auch ohne Kenntnis des Sourcecodes manipuliert werden könnte [Siet06].

[58] Eine *Dedicated Special Purpose Machine* ist eine Maschine, die ausschließlich zu einem bestimmten Zweck verwendet werden kann und die Verwendung zu einem anderen Zweck, als dem dedizierten, ist nicht möglich

5.4.2.6 Authentizität des Sourcecodes

Andere Sicherheitsaspekte betreffen den Softwareentwicklungsprozess wie auch den Update-Prozess der Software auf einer Wahlmaschine [MaSt05].

Der Update-Prozess einer Software birgt ein hohes Sicherheitsrisiko, da durch eine solche Schnittstelle im Zuge des Updates zusätzlicher Code eingebaut oder bestehender Code verändert werden kann. Durch eine derartig offene Schnittstelle zur Software können Angreifer bösartigen Code platzieren, Hintertüren einbauen und auf diese Art das Wahlergebnis manipulieren.

Ein weiteres Problem betrifft den verwendeten Compiler. So ist es möglich, dass Sourcecode, der alle Reviews übersteht, auf einer Maschine mit einem bösartigen Compiler compiliert wird. Das Ergebnis ist ein manipuliertes Programm, obwohl der Sourcecode nicht geändert wurde und authentisch ist. Dasselbe Problem betrifft das Betriebssystem, auf dem zum einen entwickelt und zum anderen die Software eingesetzt wird.

Beim Kopieren und Updaten des Sourcecodes auf der Wahlmaschine muss auch dessen Authentizität überprüft werden. Werden etwa keine Signaturen und Prüfsummen-Verfahren zur Kontrolle verwendet, um zu gewährleisten, dass das übertragene Programm auch dem Erwarteten entspricht, kann manipulierter Code eingeschleust werden.

Weitere Risiken bei E-Voting-Systemen entstehen durch integrierte Sicherheitsüberprüfungen der Hard- und Software. Eingebaute Überprüfungen, die etwa per Knopfdruck durchgeführt werden, können zusammen mit der Hard- oder der Software so manipuliert werden, dass sie wieder ein korrektes Ergebnis liefern. Werden externe Überprüfungsmechanismen verwendet, sinkt das Risiko, dass die Überprüfung sabotiert wurde.

5.4.2.7 Anzahl der Stimmen

Ein wesentlicher sicherheitskritischer Punkt ist, dass die Anzahl der autorisierten mit der Anzahl der abgegebenen Stimmen übereinstimmen muss. In Sarpy County, Nebraska, in den USA kam es bei den Wahlen 2004, dazu, dass 10.000 zusätzliche Stimmen gezählt wurden, obwohl weniger als 3.000 Wähler in diesem Wahlkreis registriert waren [WOWT04]. Diese Unstimmigkeiten waren auf menschliches Versagen zurückzuführen, da der Fehler eines Technikers dazu führte, dass Wahlkarten von Wählern aus anderen Wahlkreisen (Absentee Ballots) doppelt gezählt wurden.

Ein weiterer derartiger Vorfall ereignete sich im selben Jahr im Bezirk Columbus in Ohio, USA, bei dem 3.893 zusätzliche Stimmen dem Kandidaten Bush zugeordnet wurden, obwohl nur 800 Wähler registriert waren. Der Mangel entstand beim fehlerhaften Auslesen der Endergebnisse [Schw04]. Unstimmigkeiten bei der Anzahl der Stimmen gab es ebenfalls 2004 in Franklin County, Ohio, wo 4.258 Stimmen für den Kandidaten Bush im Vergleich zu 260 Stimmen für den Kandida-

ten Kerry gezählt wurden, obwohl nur insgesamt 638 Wähler ihre Stimme abgegeben hatten [Zett04].

Umgekehrte Vorkommnisse, bei dem Stimmen verloren wurden, traten zum Beispiel 2004 in Carteret County, North Carolina, USA auf. Mehr als 4.500-12.000 Stimmen (die Zahl unterschied sich je nach Quelle in der Presse) gingen aufgrund einer Fehlfunktion der Wahlmaschine verloren. Die Maschine war für die Speicherung einer geringeren Anzahl an angegebenen Stimmen ausgelegt und als die Speicherkapazität überschritten wurde, hatten neu gespeicherte Stimmzettel die bestehenden überschrieben. Das System konnte pro Tag maximal 3.005 Stimmen speichern, obwohl es laut Herstellerangaben 10.500 sein sollten. Die Stimmen, die nicht mehr gespeichert werden konnten, gingen so für immer verloren [USAT04].

In Napa County, California, USA, wurden ebenfalls 2004 6.692 Stimmen von Auslandswahlkarten wegen eines Kalibrierungsfehlers des optischen Scanners nicht gezählt, weil dieser unterschiedliche Tinten nicht erkennen konnte. Da es sich aber um einen Scanner für Papierstimmzettel handelte, konnte eine erneute Zählung gestartet werden, die alle Stimmen erfasste [Zett04a].

2000 sollen dem Kandidaten Al Gore in Volusia County, Florida, sogar 16.022 Stimmen abgezogen worden sein [Film1][59]. Bei der Wahl 2000 in Florida wurden Lochkartensysteme und keine DRE-Wahlmaschinen eingesetzt.

Bei der Kongresswahl im Herbst 2006 in Florida, im Landkreis Sarasota, bei denen der republikanische Kandidat mit nur 369 Stimmen Vorsprung nach der Auszählung gewann, kam es zu einem Verlust von rund 18.000 Stimmen (rund 13 % der Wähler, also jeder achten Stimme). Diese Anzahl an Stimmen wurde als Undervotes, also als ungültig, gewertet - üblicherweise kommt es in den USA zu einem Anteil von zwei bis drei Prozent an ungültigen Stimmen. Eine Prüfung der Wahlmaschinen des Herstellers ES&S wurde angeordnet, welche die Geräte testen und eventuelle Manipulationen nachweisen sollte. Die Ursache für die Abweichung sollte offiziell geklärt werden, allerdings wurde bei der Untersuchung kein Fehler gefunden.

Kritik an dieser Wahlmaschinenprüfung kam von David Dill von der kalifornischen Stanford Universität und Dan Wallach von der Rice Universität in Texas. Die Kritiker beanstandeten, dass die Aufklärung nur halbherzig durchgeführt und der Ursache nicht auf den Grund gegangen wurde. Es wurden nur zehn Geräte für eine Testwahl überprüft und der Sourcecode wurde von Wissenschaftlern des *Security and Assurance in Information Technology* (SAIT) Lab von der Florida State Universität inspiziert. Allerdings wurde die Testwahl nicht unter realistischen Bedingungen durchgeführt, mögliche Touchscreen Kalibrierungsprobleme wie auch unregelmäßige Antwortzeiten wurden außer acht gelassen und der Quellcode nur oberflächlich überprüft. Für eine eingehende Analyse hätten das Bug-Tracking System und die interne Dokumentation des Herstellers herangezogen werden

59 Eine Liste der Referenzen auf Filme ist im Anhang Appendix D zu finden.

müssen [DiWa07]. Obwohl die Ursache für die hohe Anzahl an Undervotes nicht endgültig geklärt wurde, veranlasste der neue Gouverneur Floridas Charles Christ die Abschaffung von DRE-Wahlmaschinen und die Wiedereinführung von Papierstimmzettel (mit optischen Scannern).[60]

5.4.3 Human Factors

Das Gebiet der Human Factors, also der menschlichen Aspekte und Faktoren der Sicherheitsrisiken ist ein sehr weit reichendes und geht von der Akzeptanz des Systems, über Benutzerinterfaces, bis hin zum Einfluss jedes einzelnen Individuums in jeder Phase der Erstellung, des Einsatzes und der Wartung eines E-Voting-Systems.

5.4.3.1 Akzeptanz und Vertrauen

Ein Punkt der *Human Factors* betrifft generell die Akzeptanz von E-Voting bei einer Einführung zusammen mit dem Vertrauen der Wähler in das System. Bei herkömmlichen Wahlen ist für jeden Wähler auf der Basis seiner eigenen Handlungen und Beobachtungen nachvollziehbar, ohne großartiges technisches Verständnis über den Ablauf des Wahlvorgangs aufbringen zu müssen (siehe auch Kapitel 2.2). Eine physische Repräsentation seiner Stimme existiert. Die Transparenz des traditionellen Verfahrens ist bisher unschlagbar. Jeder Bürger kann (als Wahlbeobachter oder Beisitzer) beobachten, dass nur berechtigte Wähler zur Stimmabgabe zugelassen werden, die Wahlurne während der Wahl nicht manipuliert wurde, und dass die Anzahl der abgegebenen Stimmen mit den gezählten übereinstimmt. Bei elektronischen Systemen ist es auch für einen Experten schwierig nachzuvollziehen, wohin einzelne Stimmen wandern und ob sie korrekt gezählt werden [EvPa04].

Ein weiterer Aspekt ist generell das Vertrauen der Menschen in die Technik. Soziale Funktionen (Kommunikation, Transaktionen, etc.) werden durch technische Hilfsmittel erleichtert. Somit wird auch Verantwortung abgegeben.

> „Informationsverarbeitung und Kommunikation werden dadurch vom Funktionieren einer Technik abhängig, auf die sich die Menschen verlassen. Im Vertrauen auf die Technik erhöhen sie deren Leistungsfähigkeit - und damit zugleich das Schadenspotenzial.“ [RoWe89, S. 7]

Dritte haben so die Möglichkeit, in diese vom Menschen entkoppelten Prozesse einzugreifen und diese leichtfertig und missbräuchlich zu gefährden.

[60] Über weitere Missstände und Irregularitäten wird in der Dokumentation „Uncounted - The New Math of American Elections“ von Earnhardt [Film3] berichtet.

Notwendig sind breite, öffentliche Diskussionen, die verhindern, dass ein unreflektierter Technikoptimismus vollendete Tatsachen schafft, die später zu bedauern wären. Alternative Entwicklungsmöglichkeiten sollten bedacht und eingesetzte Systeme möglichst über lange Zeit getestet werden. Politische Rahmenbedingungen wie gesetzliche Vorgaben, technische Normung und Zulassungsverfahren sind notwendig, um die Verletzlichkeit der „Informationsgesellschaft“ zu reduzieren [RoWe89, S. 247].

Bei einer Einführung von E-Voting sollte der bestehende Grad des Vertrauens in das gegenwärtige Wahlverfahren beibehalten werden. Davon betroffen ist E-Government im Allgemeinen, wie auch der E-Voting-Prozess. Das Vertrauen der Bürger kann durch Einführung expliziter, verständlicher Sicherheitsmaßnahmen unterstützt werden [XeMa04a].

5.4.3.2 Fehler von Individuen

Ein weiterer entscheidender Punkt ist der Einfluss jedes Individuums in jeder Phase der Her- und Bereitstellung der E-Voting-Maschinen, der Entwicklung der Soft- und Hardware, bis hin zum Versenden des Wahlergebnisses jedes Sprengels an eine zentrale Stelle.

James Reason unterscheidet zwei Fehlervarianten im menschlichen Verhalten: aktive Fehler und latente Fehler. *Aktive Fehler* von Menschen (als Bediener eines Systems) wirken sich hierbei unmittelbar auf das System aus. *Latente Fehler* werden von Menschen, die am Entwurf, Design oder an Entscheidungen der Leitung beteiligt sind, oder durch mangelhafte Ausstattung, überarbeitetes Personal, zeitlichen Druck oder Kommunikationsfehler erzeugt. So können diese lange Zeit ruhen, bis sie zusammen mit anderen Faktoren die Systemabwehr durchdringen. Latente Fehler stellen für die Sicherheit eines komplexen Systems die größere Bedrohung dar [Reas94, S. 216].

Aktive menschliche Fehler bei E-Voting-Systemen können zum Beispiel eine fehlerhafte Aufstellung der Wahlmaschinen oder die falsche Eingabe von Daten bedeuten. Latente Fehler können sich von einem schlechten Entwurf, bis hin zu Programmierfehlern erstrecken. Da auch hier latente Fehler eine größere Gefahr darstellen, ist es hier besonders wichtig, das Augenmerk auf die Vermeidung dieser zu richten. Dies kann durch stetige Qualitätskontrollen, Reviews und Usability Studien erreicht werden.

Bereits beim Softwareentwicklungsprozess sind viele Sicherheitsrisiken denkbar. Der Programmierer kann, falls es keine oder unzureichende Code-Reviews geben sollte, bösartigen Code, wie z. B. Hintertüren, absichtlich oder unabsichtlich einbauen, die unbemerkt bleiben können. Beim Versenden der Teilergebnisse aus den Wahlsprengeln ist denkbar, etwa auf eine Man-In-The-Middle Attacke zu stoßen.

Durch paarweises, alternierendes Entwickeln der Software wird der Einfluss eines (bösartigen) Mitarbeiters beschränkt. Zusätzliche externe oder interne Reviews, Tests und Zertifizierungen schützen den gesamten Softwareentwicklungsprozess vor „gekauften“ Beschäftigten.

Allerdings müssen diese Fehler nicht unbedingt absichtlich geschehen, denn es ist menschlich Fehler zu machen:

„[..] humans will inevitably make errors when they build something new.“ [Schu03a]

Sicherheit wird immer von Menschen in Systemen implementiert, die von Menschen entworfen wurden. Somit wird die IT-Sicherheit signifikant durch den menschlichen Faktor beeinflusst.

5.4.3.3 Lagerung der Maschinen

Kurz vor der Aufstellung von Wahlmaschinen werden oft die Sicherheitsmaßnahmen verschärft, aber in den Jahren zwischen den Wahlen sinkt die Sicherung der Geräte bei der Lagerung erheblich und die Maschinen stehen fast offen und bereit zur Manipulation.

Ed Felten, Professor an der Universität Princeton, schrieb in seinem Weblog[61] über die mangelhafte Sicherung der Wahlmaschinen an den Tagen vor den Kongresswahlen in den Vereinigten Staaten 2006. Die Maschinen standen unbewacht, ungesichert und somit offen für Manipulationen auf dem Gang eines Wahlbüros am Wochenende vor dem Wahltag (siehe Abbildung 17).

[61] http://www.freedom-to-tinker.com

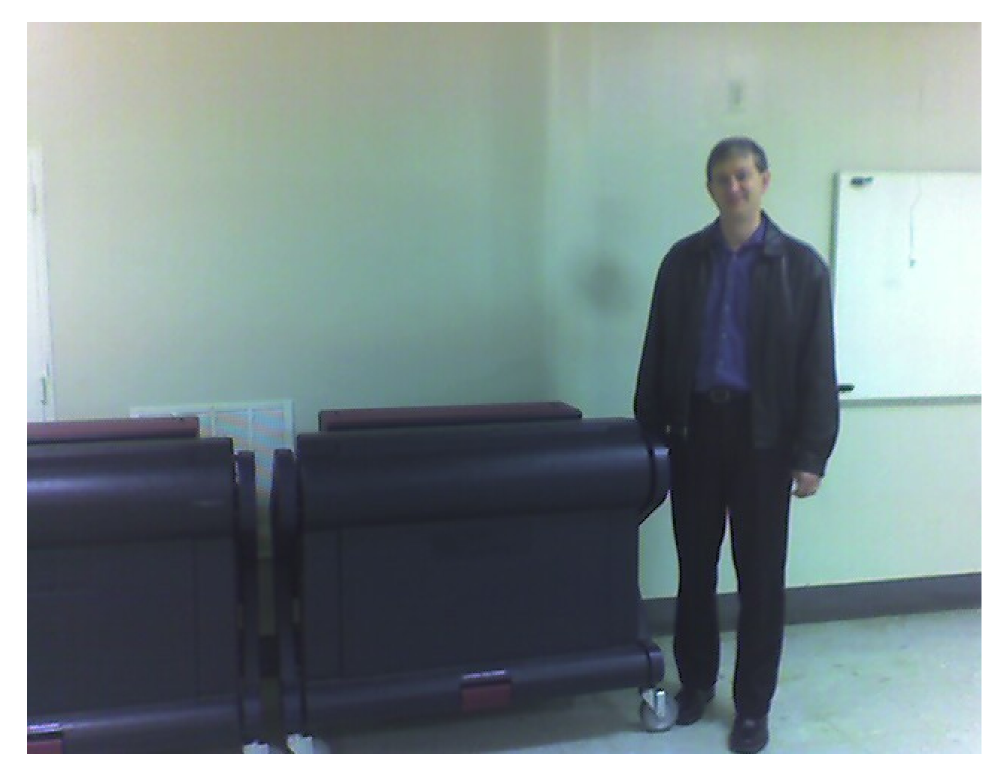


Abbildung 17: Ed Felten bei ungesicherten Wahlmaschinen, Quelle http://www.freedom-to-tinker.com

Jede beliebige Person, die sich am Vorwahltag in den Wahlbüros aufgehalten hat, hätte sich an den Maschinen zu schaffen machen können.

5.4.3.4 Usability

Unter *Usability* (zu Deutsch „Bedienbarkeit" oder „Gebrauchstauglichkeit") versteht man das Ausmaß, in dem ein Produkt von einem bestimmten Benutzer verwendet werden kann, um bestimmte Ziele in einem bestimmten Nutzungskontext effektiv, effizient und zufriedenstellend zu erreichen [aus DIN EN ISO 9241-11:1999].

Die Usability für Wähler, aber auch für Wahlhelfer ist ein entscheidender Punkt beim Einsatz von E-Voting-Systemen und stellt ebenfalls ein Sicherheitsrisiko dar [HoBe00]. Die in Kapitel 5.4.1 bereits erwähnte Studie, die die Genauigkeit von Diebold-Wahlmaschinen hinterfragte, stellte fest, dass ein Drittel der Wahlhelfer Probleme beim Aufsetzen der Wahlmaschinen hatte, 45 % hatten Probleme beim Abschluss der Maschinen, 38 % hatten Probleme mit den Druckern [Song06]. Dieselbe Studie zeigte auch, dass 90 % der Wähler das neue System mochten, allerdings 10 % der Wähler mit den Maschinen ebenfalls Probleme hatten.

Die grafische Benutzerschnittstelle birgt ebenfalls ein hohes Sicherheitsrisiko, da die Gestaltung des Stimmzettels (Platzierung von „wichtigen" Abstimmungen im oberen Bereich der Anzeige, „un-

wichtige“ weiter unten, oder umgekehrt, eine Blättern-Funktion, etc.) die Wahlentscheidung beeinflussen. Die Skalierung eines Touchscreen-Monitors ist ebenfalls ein Angriffsziel, denn wenn Skalierung und Kalibrierung mit dem angezeigten Stimmzettel nicht korrelieren, kann es zu falschen Ergebnissen kommen [SaKo06].

Bei der Konstruktion der Geräte, wie auch bei der grafischen Gestaltung, muss auf eine allgemeine Verständlichkeit, besonders für Technik-unbewanderte oder ältere Menschen Wert gelegt werden. Versuche an der Paul Verlaine Universität in Metz, Frankreich, zeigten in diesem Bereich starke Probleme. Bei Untersuchungen mit einigen der Maschinen, die für die Präsidentschaftswahl in Frankreich eingesetzt wurden, konnten vier von sieben Personen, die älter 65 Jahre waren, ihre Stimme nicht abgeben.

Das elektronische Vorfallsmelde-System EIRS (Election Incident Reporting System), das seit 2004 in den USA eingesetzt wird, um Irregularitäten vor, während oder nach der Wahl festzuhalten, enthält zum derzeitigen Zeitpunkt über 42.000 gemeldete Ereignisse [Lope05]. In diesem System werden organisatorische Mängel festgehalten, wie auch Probleme beim Umgang mit den Wahlmaschinen (Usability) oder Fehler bei der Stimmabgabe.

Ein weiteres Problem sind die sogenannten *Butterfly Ballots* (zu Deutsch wörtlich „Schmetterlings-Stimmzettel“), wie sie in Palm Beach, Florida, bei den Wahlen im Jahr 2000 eingesetzt wurden (siehe Abbildung 18). Das Lochkartensystem sah vor, dass das Loch neben der gewählten Partei ausgestanzt werden solle, allerdings kam es durch die versetzte Auflistung der Parteien und Darstellung der Stellen, an denen gestanzt werden sollte, dazu, dass einige Wähler, die für die Demokraten stimmen wollten, die Reform-Partei gewählt haben [Over06, S. 54f].

Ähnliche Probleme gab es im Jahr 2000 in Chicago / Cook County, wo ein ähnlich missverständlicher Stimmzettel verwendet wurde (siehe Abbildung 19, oben). Eine Usability-Studie, durchgeführt von Marcia Lausen, ergab, dass die Namen der Kandidaten schwer zu lesen waren, die Felder für das Abstimmen zu nahe zusammen standen, und die Aufteilung der Kandidaten im Layout unzureichend war [Laus07, S. 17f]. Der untere Teil der Abbildung 19 zeigt den Stimmzettel nach dem Redesign.

Abbildung 18: Erklärung eines Butterfly Ballot. Quelle Sun-Sentinel

Ein historisches Beispiel für ein manipulatives Stimmzettel-Design sind die Stimmzettel, die zur Zeit der NS-Diktatur bei Reichstagswahlen (die zweite Reichstagswahl 1933 und die Reichstagswahlen 1936 und 1938) eingesetzt wurden. So gab es auf dem Stimmzettel nur einen Kreis für die NSDAP, für eine Gegenstimme musste man explizit „Nein“ auf den Stimmzettel schreiben. Ein weiteres Beispiel aus dieser Zeit sind Stimmzettel mit verschieden großen Kreisen (ein Großer für „Ja“, ein Kleiner für „Nein“) bei der Volksabstimmung über den Anschluss Österreichs am 13. März 1938.

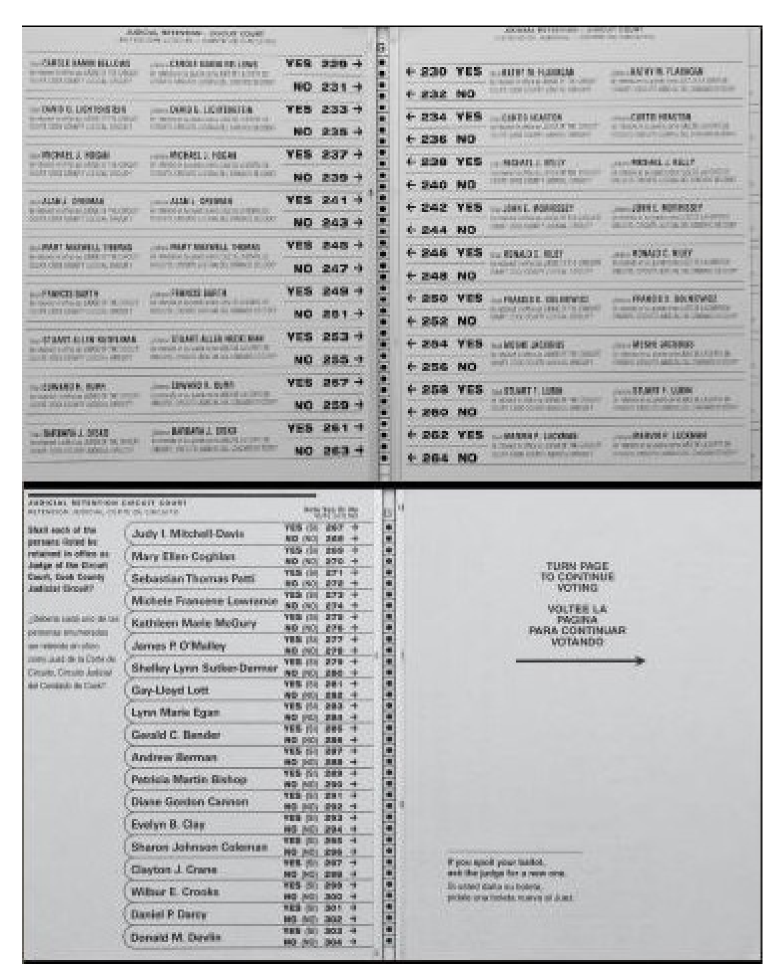


Abbildung 19: Stimmzettel aus Chicago / County, vor (oben) und nach dem Redesign (unten), Quelle [Laus07, S. 16ff.]

Ein weiteres Problem bei schlechter Usability einer Wahlmaschine ist, dass das Wahlgeheimnis gefährdet werden kann, wenn ein Wähler Hilfe von Mitgliedern der Wahlkommission anfordern muss. So könnte eine dritte Person die Stimme des Wählers einsehen, ohne dass das gewollt ist.

Durch den Einsatz von Wahlmaschinen sollte es nicht zu Verzögerungen im Ablauf kommen. Bei den Wahlen zu den Präsidentschaftswahlen in Frankreich 2007 kam es unter anderem wegen schlechter Usability dazu, dass es wegen der schlechten Aufstellung zu Wartezeiten von bis zu zwei Stunden kam [Sail07], in den USA sogar bis zu vier Stunden [Over06, S. 43].

Um Verzögerungen zu verhindern, sind verständliche Anleitungen zur Benutzung der Wahlmaschinen und zum Ausfüllen des Stimmzettels notwendig. Die beiden Beschreibungen des Ablaufes einer Stimmabgabe (siehe Abbildung 20) haben die gleiche Aussage, aber durch das Redesign der alten Anleitung (links) ergab sich eine viel klarere Vorgehensweise (rechts).

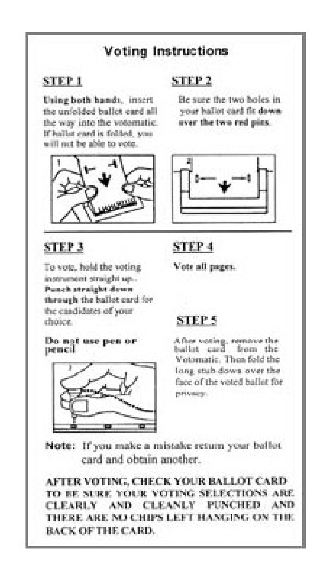




Abbildung 20: Überarbeitung einer Anleitung zur Stimmabgabe
Quelle [Ques04]

So wurden die Texte gekürzt und in eine weitere Sprache übersetzt, sowie die Schritte klarer aufgegliedert.

5.4.3.5 Administration

Das administrative Personal bei Wahlen gewinnt mit der Einführung elektronischer Wahlen immer mehr an Bedeutung. Zusätzliche Schulungen und Anreize, wie etwa ein höheres Gehalt, werden notwendig. Die Anforderungen an Wahlhelfer steigen mit der Komplexität der Wahl-Technologie, da die möglichen Fehlerfälle immer vielfältiger werden [CaBo05].

Die Mitarbeiter der Wahlkommission müssen ebenfalls über solides technisches Grundwissen verfügen, um mit Wahl-Computern umgehen, die Maschinen vor, während und nach dem Einsatz überprüfen und in Störfällen akkurat reagieren zu können. Derzeit belaufen sich die Trainingsanforderungen in den USA auf nur 4 Stunden [Ques04]. Von der Qualität des Trainings der Wahlhelfer hängt auch ab, wie gut diese ihre Arbeit verstehen und bei Wahlen Bürgern helfen können.

Beim Wahlverfahren müssen administrative Aufgaben klar definiert, Rollen gut aufgeteilt, und Verantwortlichkeiten klar ersichtlich gemacht werden. Die Abhängigkeiten zwischen einzelnen Abteilungen können zu Verzögerungen führen. 2003 kam es zu Problemen bei einem Pilot Projekt der *Second Public Authority* (PA2) in Großbritannien, wo eine Abteilung keine Zeit hatte, die Fertigstellung der Arbeitsschritte einer anderen Abteilung zu überprüfen.

Um Sicherheit zu gewährleisten, wurde in einigen Wahlstationen die erforderliche Hardware erst einen Tag vor der Wahl geliefert. Allerdings hatte das Personal, das die gelieferte Hardware über-

nommen hatte, nicht ausreichend Zeit, diese nochmals sorgfältig zu überprüfen. Somit erlaubte der straff gehaltene Zeitplan keine ausreichenden Sicherheitsüberprüfungen [XeMa05].

Ein weiterer Aspekt bei der Wahladministration ist, dass diejenigen, die die Wahl beaufsichtigen, das größte Manipulationsinteresse haben, also die Vertreter der Parteien. Derzeit ist bei Urnenwahlen eine Manipulation schwer realisierbar, da Mitglieder verschiedener Parteien in der Wahlkommission vertreten sein müssen (siehe auch Kapitel 2.2). Bei elektronischen Wahlen muss darauf geachtet werden, dass dieser Grundsatz nicht verloren geht.

5.4.3.6 Movie Plot Security

Ein weiterer menschlicher Aspekt ist die Einführung von Schutzmaßnahmen vor Angriffen, nachdem diese aufgetreten sind. Diese Eigenschaft wird im Security Fachjargon *Movie Plot Security* (geprägt vom Sicherheitsexperten Bruce Schneier) genannt. Gemeint ist, dass Sicherheitsexperten Schutz vor spezifischen Risiken erst implementieren, nachdem diese bereits von anderen ausgenutzt wurden. Neue Schutzmaßnahmen treten in erst Kraft, nachdem das Szenario (der „Film“) gesehen wurde, anstatt einen breiten, vorbeugenden Schutz vor Angriffen mit generischen Konzepten zu entwickeln.

Somit ist die wahrgenommene, gefühlte Sicherheit, die durch spezifische Sicherheitsrisiken entsteht, wie etwa Kontrolle von Schuhen vor dem Abflug am Flughafen, nicht mit der tatsächlichen Sicherheit vergleichbar. Die von der Politik vorgegebenen Richtlinien decken nur einen Teil der Sicherheitsrisiken - der *Movie Plot Threads* - ab. Doch meist sind die Bedrohungen, gegen die Maßnahmen entwickelt wurden, Sonderfälle, nicht besonders realistisch oder wahrscheinlich. Meist stellen diese Sicherheitsmaßnahmen bloß eine Beschneidung der persönlichen Freiheit (Stichwort Datenschutz und „gläserner Mensch“) dar.

Einen ähnlichen Fall stellt das *Parallel Testing* dar. Bei dieser Art des Testens von DRE-Wahlmaschinen wird am Wahltag, neben den tatsächlich eingesetzten Wahlmaschinen, eine Reihe von Maschinen zu Testzwecken aufgestellt, die einen Phantom-Wahlbezirk darstellen. Ziel ist es, durch eine Testaufstellung, welche möglichst einer normalen Aufstellung entspricht, Fehler zu entdecken, die bei den normalen Wahlbezirken auftreten können. Dabei werden laufend Testwahlen durch Testpersonen durchgeführt, die alle möglichen Aktionen gewöhnlicher Wählern mimen sollen [Sham04].

Nachteil des Parallel Testings ist, dass mit diesem Verfahren probabilistische Attacken[62], „knock" Attacken[63] und Time Trigger[64] nicht entdeckt werden. Manipulationen, die erst nach dem Ziehen der Stichprobe von Wahlgeräten wirksam werden, lassen sich mit Parallel Testing ebenfalls nicht aufdecken. Weiters ist zu entscheiden, welche Konsequenzen eine aufgedeckte Irregularität, wie etwa eine Diskrepanz bei den Testmaschinen, nach sich ziehen würde [GoHe06, S. 11].

5.4.3.7 Mangelnde Sicherheitsvorschriften

Die Sicherheitsvorschriften beim Einsatz von E-Voting-Maschinen in den USA sind weniger streng und sorgfältig als bei Glücksspielmaschinen. Besonders Insider-Attacken sind ein großes Problem, das von amerikanischen Herstellern von Wahlmaschinen außer acht gelassen wird [DiRu04]. So gibt es etwa ausführliche Hintergrund-Überprüfungen der Mitarbeiter in Kasinos, die das administrative Personal von E-Voting-Systemen nicht absolvieren muss. Test von Slot Machines (einarmige Banditen) werden in der realen Einsatzumgebung durchgeführt, bei E-Voting-Maschinen ist das meist nicht möglich. Eine staatliche Kontrolle wie bei Kasinos (etwa der Nevada Spielkommission) oder wie auch bei der Einführung von Medikamenten fehlt bei E-Voting-Systemen, da die Standards der *Federal Election Commission* nicht staatlich, etwa durch Gesetze zwangsverpflichtend, eingeführt werden (siehe auch Kapitel 6.9.2).

Oft werden Argumente für mangelnde Sicherheit so begründet, dass kein Grund oder keine Möglichkeit gesehen wird, angegriffen zu werden. Allerdings ist der (finanzielle) Anreiz für Angriffe hoch.

E-Voting-Systeme müssen entworfen werden, um niveauvollen und raffinierten Attacken entgegnen zu können, einschließlich solchen mit massiven finanziellen Ressourcen (es gibt eine hohe politische und finanzielle Motivation eine Wahl auf eine andere Mehrheit umschwingen[65] zu lassen). Überprüfungen der Maschinen und Wahlbeobachter bei der Wahl helfen gegen einige dieser Angriffe, aber nicht gegen alle.

> „The threats are real, making openness and verifiability critical to election security." [KoSc04, S. 104]

[62] Bei probabilistischen Attacken werden verschiedene Angriffsarten mit einer Wahrscheinlichkeit bewertet.

[63] „Knock" Attacken: Mit einer bestimmten Eingabekombination (Tastenkombination oder Eingabe über bestimmte Bereiche am Touchscreen in einer bestimmten Reihenfolge) wird ein bestimmter, versteckter, bösartiger Befehle ausgeführt.

[64] Time Trigger: Zu einem bestimmten Zeitpunkt werden bösartige Prozesse ausgeführt.

[65] „Umschwingen" bedeutet, die Wahl für einen anderen Kandidaten als Sieger ausgehen zu lassen.

5.4.3.8 Wahlkreismanipulation

Der gezielte Einsatz von unterschiedlichen Wahlsystemen kann zur Manipulation des Wahlkreises führen. So hat eine Studie gezeigt, dass Lochkartenmaschinen, die generell eine höhere Wahrscheinlichkeit haben, ungültige Stimmen zu produzieren (siehe Kapitel 5.4.1.1), in Regionen der USA eingesetzt wurden, in denen ein hoher Anteil an farbigen Bürger lebte [Brad04, S. 27]. So wurden diese Bevölkerungsschichten benachteiligt, die tendenziell eher Demokratisch wählen [Over-06, S. 69].

Durch speziell gewählte Öffnungszeiten der Wahllokale und Wahlkreise kann der Wählerkreis ebenfalls manipuliert werden. So können Wähler aus der Arbeiterschicht an ihrer Teilnahme behindert werden, indem etwa die Öffnungszeiten mit den Arbeitszeiten übereinstimmen. Im Bundesverfassungsgesetz Österreichs wird explizit die Wahl z. B. Nationalratswahl an einem Sonntag oder einem anderen Ruhetag vorgeschrieben [BGBl30 Art. 26a], um eine solche Manipulation zu verhindern.

Nicht nur durch Öffnungszeiten, sondern auch durch schlechte Usability können bestimmte Personengruppen (ältere Menschen, Sehbehinderte, etc.) gezielt ausgeschlossen werden (siehe auch Kapitel 5.4.3.4).

Gerrymandering[66] ist die absichtliche Verschiebung von Wahlkreisgrenzen in einem Mehrheitswahlssystem, um mehr Stimmen zu gewinnen. So kann durch gezielte Bestimmung der Grenzen ein Vorsprung für eine Partei erzielt werden, obwohl sie nach der Anzahl der Stimmen nicht gewinnen würde. In dem Beispiel in Abbildung 21 sieht man, dass, obwohl Blau in der Überzahl wäre, Rot durch die Aufteilung eine Mehrheit in zwei Bereichen hat und somit gewinnen würde.

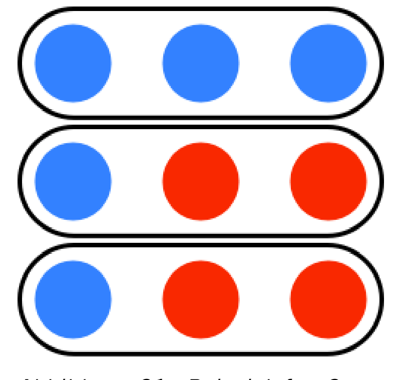


Abbildung 21: Beispiel für Gerrymandering, Quelle Wikipedia http://de.wikipedia.org/wiki/Gerrymandering

[66] Obwohl Gerrymandering nicht unmittelbar mit E-Voting in Zusammenhang steht, wird diese Form der Wahlkreismanipulation der Vollständigkeit halber erwähnt.

Als Beispiel für erfolgreiches Gerrymandering kann der US Bundesstaat Texas herangezogen werden. Bei der Wahl 2002 wurden etwa 53 % der Stimmen für republikanische Kongresskandidaten abgegeben, aber nur 47 % der Sitze im Kongress wurden von Republikanern besetzt. Mit einem erneuten Ziehen der Grenzen für die Wahl 2004 erlangten die Republikaner einen Vorsprung von 66 % der Sitze im Kongress, wobei sich die Grenzen über viele Meilen hinweg zogen und ein recht unförmiges Bild ergaben [Over06, S. 26ff].

Es gibt allerdings Algorithmen, die Gerrymandering verhindern. Diese Programme ermöglichen eine möglichst parteilose Aufteilung der Bezirke [RiSc08].

5.4.3.9 Wahlbetrug

In Österreich kam es noch zu keinem bundesweiten Manipulationsversuch von Wahlen. Auf Gemeindeebene wurde Wahlbetrug ebenfalls nicht festgestellt[67], allerdings lässt sich ein solcher Fall schwerer feststellen (siehe auch Kapitel 5.3). Die Strafen bei Wahlbetrug sind recht hoch und befinden sich im Rahmen einer Freiheitsstrafe von bis zu drei Jahren [BGBl74, § 262 - § 268].

Dezidiert konnte Wahlbetrug mit E-Voting-Systemen noch nicht eindeutig nachgewiesen werden. Die Motivation dafür ist allerdings groß und die Auswirkungen eines Anschlages eines Einzeltäters können enorm sein (siehe auch Kapitel 5.2).

In einem Fall behauptet Clint Curtis im Jahr 2000 als leitender Programmierer einer Firma in Florida beauftragt worden zu sein ein „Vote Stealing"-Programm für DRE-Wahlmaschinen zu entwickeln, mit dem man beliebig viele Stimmen einem gewünschten Kandidaten zuordnen kann. Beauftragt wurde er von einem damaligen repräsentantischen Abgeordneten, der ebenfalls nebenberuflich für die Firma arbeitete. Curtis dachte damals, die Software sollte dazu dienen, um auf Risiken hinzudeuten, allerdings erfuhr er dann, dass das Programm in West Palm Beach für die Republikaner eingesetzt werden sollte, worauf er sich an die CIA, das FBI und andere Behörden wandte. Da die Behörden eher hinhaltend ermittelten, wandte sich Curtis 2004 an die Öffentlichkeit, wobei der vermeintliche Auftraggeber alles bestritt [Film3].

5.4.3.10 Beeinflussung der Hersteller

Dem Hersteller Diebold wird ein nahes Verhältnis zur republikanischen Partei nachgesagt. Die Dokumentation Film „Hacking Democracy" [Film1] setzt sich ebenfalls mit diesem Thema auseinander. Diebolds CEO Walden O'Dell schrieb, während er sich für die Wiederwahl-Kampagne für George W. Bush einsetzte, einen Brief an potentielle Spender:

[67] Quelle: Telefonat mit Mag. Robert Stein, Bundesministerium für Inneres, Sektion III - Recht, Abt. III/6 - Wahlangelegenheiten vom 17.4.2008.

„committed to helping Ohio deliver its electoral votes to the president." [LaMo04]

Die Firma Diebold hat ihren Sitz in North Canton, Ohio. Derartige Aussagen lassen Zweifel an der politischen Unabhängigkeit der Wahlmaschinen-Hersteller offen.

6 Maßnahmen

In diesem Kapitel werden verschiedene Maßnahmen zur Gewährleistung der Sicherheit von E-Voting-Systemen vorgestellt. Diese reichen von allgemeiner Qualitätssicherung, über Normen und Zertifizierungen, bis hin zu Prüfverfahren.

6.1 Allgemeine Sicherheitsanforderungen

Folgende Kriterien für essenzielle Anforderungen an elektronische Wahlsysteme (diese werden auch als die „6 Gebote“ bezeichnet) werden hier [Sham93] als Regeln gegeben:

I. Jede Stimme bleibt ein unantastbares Geheimnis.
II. Jeder Wähler darf nur einmal abstimmen und nur für jene Parteien, für die der Wähler autorisiert ist.
III. Das System darf nicht manipulierbar sein.
IV. Die Stimmen müssen genau gezählt werden.
V. Das System muss während der gesamten Wahl verfügbar sein.
VI. Ein Audit Trail soll verfügbar sein, um Verstöße gegen die Regeln II-IV zu erkennen, er darf aber nicht Regel I verletzen.

Diese allgemeinen Grundsätze gelten für Urnenwahlen wie auch für E-Voting-Systeme und stimmen mit den rechtlichen Bestimmungen überein (siehe auch Kapitel 2.1).

Eine weitere Liste der allgemeinen Sicherheitsanforderungen an E-Voting-Systeme wird hier gegeben (Auszug): [Schl00, S. 18ff]

- Authentifikation des Wählers
- Autorisierung: Zugriffskontrolle
- Integrität der Übertragung: geschützte Kommunikationsinfrastruktur mit Kryptografie
- Korrektheit der Auszählung / des Resultates
- Verifizierbarkeit: Prüfung durch unabhängige Dritte oder die Öffentlichkeit
- Vertraulichkeit
- Nichtvermehrbarkeit: keine Wahlscheinvermehrung
- Nichtbeeinflussbarkeit: Zwischenresultate sollen nicht fälschbar sein
- Wahlgeheimnis: Entscheidungsfreiheit
- Unmittelbarkeit: Beeinflussung der Stimme

- Einhaltung der Systemanforderungen
  - Menschliche Aspekte
  - Organisatorische Anforderungen
  - Bereitstellung zusätzlicher Mittel

Diese Liste ist ein guter Ansatz, allerdings ist sie nicht ganz vollständig, da sie sich nur auf die Hardware und Software konzentriert. Menschliche Facetten, wie z. B. Insider Attacken werden nicht berücksichtigt (siehe dazu mehr in Kapitel 7).

6.2 Open-Source Peer-Reviews

Ein in der Softwareentwicklung und in der Wissenschaft gängiges Mittel zur Qualitätssicherung sind Peer-Reviews, neben Inspektionen, Walkthroughs, statistischen Analysen, Programmkorrektsheitsbeweisen und Tests [Boer04, S. 76ff]. Dabei werden die einzelnen Bestandteile des Software-Projekts (Konstruktionsunterlagen, Spezifikation, Sourcecode, Dokumentation, etc.) durch Experten, etwa Kryptografen und Sicherheitsexperten eines anderen Unternehmens des gleichen Fachbereichs, überprüft. Es gibt mehrere positive Auswirkungen von Peer-Reviews auf den Software-Herstellungsprozess. Aus Transparenz entwickelt sich automatisch Sicherheit, da das Programm von Anfang an sicherer entwickelt wird (z. B. werden daher eher asymmetrische Verschlüsselungen verwendet als statische Passwort-Überprüfungen). Der Code wird von Beginn an klarer und besser kommentiert geschrieben, wenn die Programmierer wissen, dass der Code öffentlich verfügbar gemacht wird. Fehler können auch von Dritten gefunden und korrigiert werden, Sicherheitslücken werden durch Überprüfung von Dritten aufgedeckt.

Zum einen arbeitet ein Entwickler anders, etwa aufmerksamer und besser dokumentiert, wenn er davon ausgehen muss, dass seine Arbeit nochmals überprüft werden wird. Zum anderen werden die Konzepte und Prozeduren ein weiteres Mal extern überprüft. Diese Maßnahme ist auch beim Entwurf und der Realisierung der Hardware von E-Voting-Systemen sinnvoll [Kitc04].

Offenheit in der Softwareentwicklung (*Open-Source*) ist ein Prinzip, das in vielen Software Projekten angewendet wird. Hersteller von Wahlmaschinen-Software beharren aber meist auf proprietärer Software, die nicht offengelegt wird, da gefürchtet wird, dass Sicherheitslücken oder Betriebsgeheimnisse ausspioniert werden könnten. Die Überzeugung, dass die Geheimhaltung des Quellcodes eines Systems zu mehr Sicherheit führt, ist als *Security by Obscurity* bekannt (siehe auch Kapitel 5.4.2.1). Diese Ansicht bietet allerdings eine Reihe zusätzlicher Angriffspunkte, wie etwa die fehlende Überprüfung durch unabhängige Dritte oder dass die Quellcodequalität leidet [MeNe03]. Zudem lassen sich Angreifer selten durch geschlossenen Quellcode hindern, da durch *Reverse Engi-*

neering die Funktionsweise und der innere Aufbau eines Systems auch ohne exakte Kenntnis des Soucecodes herausgefunden werden kann.

Sicherheit, die auf Geheimhaltung oder Verschleierung von Informationen beruht, ist nicht ausreichend. Eher sollten „starke“ Kryptografie-Algorithmen und andere Techniken verwendet werden, da davon auszugehen ist, dass der „Feind“ das System kennt (Shannons Maxime: „The enemy knows the system“, eine Abwandlung des Kerckhoffs Prinzip[68]). In diesem Zusammenhang wird oft Linus' Law zitiert (erstmals durch Eric Raymond geprägt):

„Given enough eyeballs, all bugs are shallow.“ [Raym01, S. 8]

Abgesehen von statischen Prüfungen wie Peer-Reviews, sind Software Tests ein elementarer Bestandteil zur Qualitätssicherung in der Softwareentwicklung. Diese dynamischen Prüfungen, unterschieden in Blackbox-Tests und Glassbox- (oder Whitebox-) Tests, überprüfen (oft auch automatisiert) den Sourcecode der Software. Diese Tests sind reproduzierbar, objektiv und lassen sich mehrfach nutzen. Weiters wird die Zielumgebung bei diesen Tests mitgeprüft und es lässt sich so das Systemverhalten sichtbar machen [FrLu04, S. 22].

Eine Möglichkeit auch vom Hersteller nicht bedachte Sicherheitslücken aufzudecken, sind neben Peer-Reviews Veranstaltungen, bei denen die Maschine von verschiedenen Sicherheitsexperten auf Herz und Nieren durch verschiedene Angriffsszenarien getestet wird. Solche Veranstaltungen können *Capture The Flag*-Wettbewerbe oder die Aufstellung eines Red Teams sein, die zum Ziel haben, Sicherheitslücken und andere Vulnerabilitäten in den untersuchten Systemen zu finden. So wurden etwa Diebold Maschinen durch ein Red Team untersucht [RABA04], das die gefundenen Sicherheitslücken des Rubin Reports [KoSt04] bestätigte und weitere fand.

6.3 Studien und Analysen

Neben den in Kapitel 5.4.2.3 erwähnten Analysen von Aviel Rubin und Dan Wallach [KoSt04], Edward Felten und Alex Halderman [FeHa06], der von Debra Bowen angeordneten Untersuchung [Bowe07, Bowe07a, Bowe07b] und den Analysen des *Chaos Computer Club* [CCC06, KuRi07] wurden zahlreiche, weitere Studien von E-Voting-Systemen durchgeführt.

Dan Wallach, Professor an der texanischen Rice Universität, hat im Rahmen seines *Hack-a-vote* Projekts ein zu Testzwecken selbst geschaffenes E-Voting-System (ein vereinfachtes DRE-Wahlsystem) von mehreren Teams von Studenten analysieren lassen. In der ersten Phase sollten die Stu-

[68] Auguste Kerckhoffs formulierte bereits 1883 folgendes Prinzip: „Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.“ [Kerc83]

denten ein Trojanisches Pferd[69] in das E-Voting-System einschleusen, in der zweiten Phase modifizierten die Studenten die Software und die Änderung sollte von Mitgliedern anderer Teams gefunden werden und in der dritten Phase sollte ein Kryptografie-Sicherheitsproblem behoben werden. Durch diesen Versuch wollte Wallach zeigen wie einfach es ist ein System zu manipulieren, welche verschiedenen Möglichkeiten Angreifer haben das zu tun, welche Wege es gibt, die Manipulation nicht erkennen zu lassen und wie schwer es auf der anderen Seite ist, Fehler zu finden und auszubessern [BaPr04].

Ein ähnliches Projekt wurde an der Johns Hopkins Universität veranstaltet: Im Rahmen einer Lehrveranstaltung wurde das Projekt *Hiding and Finding Malicious Code* ausgetragen, bei dem Studenten unter Leitung von Aviel Rubin bösartigen Soucecode in gutartigen schmuggeln sollten, andere Studenten sollten diesen versteckten Code dann wieder finden. Das Experiment zeigte, dass es viel leichter ist bösartigen Code versteckt einzuarbeiten, als jenen wieder zu finden [Woeh04].

Das *Brennan Center* führte eine der umfassendsten Studien über E-Voting-Maschinen durch, die drei Gerätetypen umfasste: optische Scanner und Touchsceen-Wahlmaschinen mit und ohne Paper Trail. Die Analyse verfolgte einen ganzheitlichen Ansatz, bei dem vier Teams jeweils einen Aspekt der Geräte untersuchen sollten. Das Usability-, das Barrierefreiheit- und das Kosten-Team untersuchten E-Voting-Systeme mit Fokus auf deren jeweiliges Spezialgebiet. Weiters analysierte das Security-Team, bestehend aus Wissenschaftlern des amerikanischen *National Institute of Standards and Technology*, David Dill, Howard Schmidt und Ronald Rivest, Sicherheitsprobleme der Wahlmaschinen, und fand mehr als 120 Risiken. Nach 18 Monaten Analyse wurde ein Bericht [Bren04] veröffentlicht, der Empfehlungen für die Steigerung der Zuverlässigkeit durch Entwicklungsmaßstäbe und Begutachtungen von E-Voting-Systemen umfasst [Over06, S. 188ff].

6.4 Kryptografie

Ein Mittel, um die Veränderung des Sourcecodes zu verhindern, ist auch hier der Einsatz digitaler Signaturen. So wird gewährleistet, dass der zum Einsatz kommende Sourcecode nicht verändert wurde. Hash-Prüfsummenverfahren genügen hierbei nicht allein, da es auf unterschiedlichen Betriebssystemen zu verschiedenen Hash-Werten kommen kann.

Generell ist der Einsatz von (blinden) digitalen Signaturen (siehe Kapitel 4.4.1), Zertifizierungen zur Authentifizierung, Autorisierung, Signatur und anderen kryptografischen Mitteln derzeit der aktuelle Stand der Technik und gilt als hinreichend sicher - da (fast) nicht brechbar - und sollte auch Anwendung finden. Allerdings ist die Sicherheit etwa verschlüsselter Dokumente für die Zukunft unsicher, da unklar ist, ob die heute gängigen Verschlüsselungsverfahren in einigen Jahren durch un-

[69] Ein Trojanisches Pferd ist eine Hintertüre in einem Software-System.

vorhersehbare, wie auch durch vorhersehbare Faktoren, wie die steigende Rechenkapazität der Computer, nicht gebrochen werden könnte.

Weiters sollten die eingesetzten kryptografischen Algorithmen ebenfalls offen und überprüfbar sein.

> „[..] the implementation of the algorithm in software and/or hardware must also be demonstrated to be correct through rigorous, end-to-end provability. Under the Common Criteria program, satisfaction of these constraints would require certification at Evaluation Assurance Level 7, which no product has yet attained.“ [Merc05, S. 18]

6.5 Security through Transparency

Das *Öffentlichkeitsprinzip* (siehe auch Punkt „Öffentlicher und transparenter Wahlvorgang“ im Kapitel 2.1) ermöglicht Kontrolle durch den Bürger. Das Prinzip besagt, dass allen interessierten Personen eine Möglichkeit geben werden muss, die Korrektheit und Sachmäßigkeit des Ablaufes und der Auszählung beobachten zu können. So kann der Verdacht einer Wahlmanipulation zerstreut werden.

Der Grundsatz der *Amtlichkeit* des Wahlprozesses sichert Kontrolle durch öffentliche Organe, wie eine Wahlkommission und Wahlbehörde. Bei E-Voting-Systemen sind diese Personen aber im Allgemeinen mangels hinreichender technischer Kenntnisse nicht in der Lage, die Software oder die Wahlcomputer zu überprüfen. Da der öffentlichen Verwaltung die technische Expertise zur Beurteilung der Risiken fehlt, verlässt sie sich meist auf Herstellerangaben und nicht-öffentliche Zulassungsverfahren. Bei der Auswahl von Wahlmaschinen für die elektronische Stimmabgabe müssen ebenso technische Experten mit einbezogen werden, die die Maschinen unabhängig inspizieren, da sonst weder Korrektheit noch Manipulationssicherheit gewährleistet werden kann (siehe auch Kapitel 6.2).

Die Möglichkeit zur Überprüfung der Gültigkeit des Wahlergebnisses, anderer Wahlgrundsätze und der Manipulationssicherheit ist bei einer Wahl mit Stimmzetteln und Urnen weit einfacher als bei einer Wahl mit E-Voting-Systemen. Elektronische Wahlsysteme gleichen einer Blackbox, in der etwas nicht Nachvollziehbares passiert. Das Speichern und das Berechnen der Wahlergebnisse sind vor dem Wähler versteckt [ORG07].

Öffenheit und Transparenz[70] bei der Stimmabgabe ist in einem demokratischen System[71] notwendig, um das Vertrauen in die Wahl und die Einhaltung der Wahlgrundsätze (siehe auch Kapitel 2.1) gewährleisten zu können. So wird durch mehr Klarheit und Einbindung der Wähler mehr Sicherheit in einem größeren Kontext gewährleistet. Durch mehr Öffentlichkeit im Wahlprozess wird die Einflussnahme durch Innen- und Außentäter minimiert, eine demokratische Teilnahme am Verlauf gewährleistet und das Vertrauen in den Entscheidungsfindungsprozess gehoben.

Bereits 1988 wurden *Audit Trails*, die die Wahl überprüfen und dokumentieren, vorgeschlagen, um die Akzeptanz zu steigern und vor verstecktem bösartigem Code (in proprietärer Software) gewarnt, der äußerst schwer zu finden ist [Salt88].

> „IT professional agree that collecting and counting votes in public elections is a highly critical computer application. Very high standards must be applied. Electronic voting must be transparent and trustworthy. The more reliable, and less polemic, systems already implemented throughout the world are open“ [Lope05]

Transparenz betrifft folgende Punkte bei E-Voting-Systemen:

- Informationen rund um die Wahl, die den Wähler bei der Informationsbeschaffung, Meinungsbildung und Entscheidungsfindung unterstützen sollen, sollen öffentlich uneingeschränkt verfügbar sein
  - Informationen zu Eckdaten: Ort und Öffnungszeiten der Wahllokale, welche Kandidaten oder Parteien werden aufgestellt etc.
  - Einsicht ins Wählerverzeichnis (Wählerevidenz) und Zuordnung des Wählers zu Wahlsprengeln
- Zugang zur Hard- und Software der Wahlmaschinen (Zertifizierungen der Geräte (mit Einsicht in das Testprotokoll), Peer-Reviews des Sourcecodes, etc.) und zugehöriger Dokumentation. Freigabe der Testberichte für die Öffentlichkeit
- Ein öffentlich diskutierbares Wahlprotokoll
- Überprüfbarkeit der kryptografischen Unterstützung

[70] Im Bericht des Software- bzw. System Design versteht man unter *Transparenz* das Verstecken der Architektur vor dem Benutzer [Tane95, p 22ff], wie zum Beispiel, dass Fehler abgefangen werden, bevor sie einem Benutzer angezeigt werden. Unter Transparenz im Zusammenhang mit Sicherheit von E-Voting-Systemen ist eine demokratische Offenheit gemeint, bei der die Öffentlichkeit die Möglichkeit hat, den Wahlvorgang mitzuverfolgen.

[71] In einem totalitären System sind die Anforderungen an ein Wahlsystem anders als in einer Demokratie.

- Möglichkeit der Wahlbeobachtung vor, während und nach der Wahl (Anwesenheit bei der Auszählung und bei der Übermittlung der Stimmen zur zentralen Wahlbehörde sind umstritten)
- Übereinstimmung der abgegebenen Stimmen mit der Summe der gezählten Stimmen (zusätzliche unabhängige Zählung der Wähler, die das Wahllokal betreten und verlassen)
- Vergleich der Wahltagsbefragungen (*Exit Polls*) vom aktuellen und der vorangegangenen Jahre
- Anonyme Papierbelege zur Validierung der abgegebenen Stimme (siehe Kapitel 6.7.1) und als Kopie zum manuellen Auszählen der Ergebnisse
- Anonyme Überprüfung der abgegebenen Stimme nach der Stimmabgabe bei der Veröffentlichung der Wahlergebnisse (öffentliches Bulletin Board, siehe auch Kapitel 6.7.2). Mit einer zusätzlichen Funktion können die anonymen Wähler dem verglichenen Ergebnis zustimmen oder es anzweifeln. Je mehr Wähler ihrem abgegebenen Ergebnis zustimmen, desto vertrauenswürdiger ist das Gesamtergebnis. Hierzu gibt es Toleranzgrenzen, die aufzeigen, ob das Wahlergebnis verfälscht wurde oder ob es als rechtskräftig von den Wähler anerkannt wird.
- Endergebnisse auf mehreren Kanälen veröffentlichen

Weiters kann Transparenz auch durch andere Verfahren wie duales Aufzeichnen (Speichern der Stimme auf mehren unterschiedlichen Trägermedien) oder sogenannte *Witness Systeme* erreicht werden. Die Witness Systeme zeichnen das Eingabegerät (wie etwa eine Tastatur) und den Bildschirm auf und dienen so als Nachweis, dass die Stimme auch so, wie sie eingegeben wurde, aufgezeichnet und gespeichert wurde. Ein Risiko dieser Methode besteht darin, das geheime Wahlrecht zu verletzen, da durch Aufzeichnungen eventuell ein Rückschluss auf den Wähler möglich sein kann.

Das Wahlgeheimnis könnte auch durch andere Hinweise auf den Wähler gefährdet werden, etwa durch fortlaufende Seriennummern auf den Stimmzetteln. Es wäre durch Notieren des Erscheinens der Wähler eine chronologische Abfolge nachvollziehbar, wobei so die Stimme zur Person zugeordnet werden könnte.

Mit den vorgestellten Punkten kann zusätzliche Transparenz so das Vertrauen in den gesamten elektronischen Wahlvorgang steigern. Dieser Ansatz zeigt eine konstruktive Art elektronische Mittel einzusetzen, um den Wahlvorgang statt proprietär (oder obskur) offener zu gestalten.

„Man gewinnt immer, wenn man erfährt, was andere von uns denken.“ (Johann Wolfgang von Goethe) [Goet17]

Lynn Landes geht in ihrem *The Landes Report: To Congress* [Land07] sogar noch einen Schritt weiter und zeigt auf, dass viele Probleme durch das Wahlgeheimnis entstehen. Demokratie bestün-

de nicht auf geheimen Wahlen, sondern, im Gegenteil, auf der Offenheit von Wahlen. Sie plädiert für mehr Vertrauen in die eigene Überzeugung und fordert offene Wahlen *ohne* Wahlgeheimnis. Ihr Bericht richtet sich an den Kongress der Vereinigten Staaten, wird aber im Allgemeinen eher kritisch aufgenommen.

6.6 Wähler-zentrierter Ansatz

Ausgangspunkt für einen wähler-zentrierten Ansatz ist *User Centered Design* (UCD), das einen auf die Benutzer ausgerichteten Entwurf eines Produktes nahe legt [ISO 13407: Human-centred design process].

In einer Arbeit über E-Voting in Brasilien [Rodr06] wird ein solcher Ansatz vorgestellt, der offenerer ist und den Wähler mehr einbindet. Eine Wähler-getriebene Wahlsystem-Entwicklung passt sich an die Wünsche und Bedürfnisse der Wähler an. Der öffentliche Dialog mit dem Wähler ist beim Entwickeln eines E-Voting-Verfahrens notwendig, um offene Demokratie zu gewährleisten.

Der Entwurf elektronischer Wahlsysteme sollte sich nicht nur auf die Stimmabgabe und -zählung fokussieren, sondern den Wähler in den demokratischen Prozess einbinden, somit soll ein *Voter Support System* geschaffen werden. Bei diesem Ansatz wird das E-Voting-System in einem weiteren Rahmen, als Informationssystem, betrachtet. Wähler werden beim Informationsbeschaffungs-, Meinungsbildungs- und Entscheidungsfindungsprozess ebenso unterstützt, wie bei der Wahl selbst und danach (Stichwort Nachverfolgbarkeit) [Robe05].

6.7 Audit-Verfahren

Audit-Verfahren bei Wahlen, also Überprüfungsmöglichkeiten durch Wähler, Wahlbeobachter und Wahlbeobachterinnen oder Mitarbeiter und Mitarbeiterinnen einer Wahlkommission, sind ein notwendiges Mittel, um die Korrektheit und Manipulationsfreiheit einer Wahl zu gewährleisten.

Zusätzliche technische Mittel, wie der Einsatz von End-to-End Systemen (siehe Kapitel 6.7.2) oder zusätzlichen Papierbelegen (siehe Kapitel 6.7.1), können dabei die Transparenz einer Wahl deutlich erhöhen.

6.7.1 Voter-Verified Paper Trail

Eine von vielen Seiten [Dill05, FeHa06, Grov04, Jone03, Jone05, KoSt04, Merc02, OoBe04, Ston03] geforderte Maßnahme ist der Einsatz von Kontrollbelegen, die von Wählern überprüfbar sind (*Voter-Verified Paper Trail* VVPT oder auch *Voter-Verified Paper Audit Trail* VVPAT oder *Contemporaneous Paper Replica* CPR genannt), David Dill startete zu diesem Thema eine Petition[72].

[72] http://www.verifiedvoting.org

Die Forderung verlangt zusätzlich zur elektronischen Speicherung der Stimme einen Papierbeleg, mit dem gezeigt wird, dass die Stimme, die abgegeben wurde, auch tatsächlich der entspricht, die man abgeben wollte und mit dem überprüfbar ist, ob die Stimme auch im Ergebnis enthalten ist. Dieser Kontrollbeleg kann für spätere geräteunabhängige Nachzählungen verwendet werden und dient ebenfalls zur Überprüfung der Korrektheit einzelner Maschinen. Dieses Verfahren ermöglicht bedeutungsvolle Neuzählungen und Audits und stichprobenartige Überprüfungen der Maschinen [DiRu04].

Die Vorteile eines Papierbelegs oder Papierbackups liegen auf der Hand: Er existiert dauerhaft und permanent, denn man kann ihn nicht entfernen oder manipulieren, ohne dass es dafür Spuren gibt. Für erneute, valide Auszählungen ist er unerlässlich. Papierbelege sind transparent und selbst für Laien verständlich und machen eine geräteunabhängige Verifizierbarkeit des Wahlergebnisses möglich. Die Wahl wird somit „softwareunabhängig". Der Begriff der Softwareunabhängigkeit, geprägt von R. Rivest [RiWa06], bezeichnet ein elektronisches Wahlsystem, bei dem eine bösartige Manipulation oder ein unentdeckter Fehler in der Software keine unentdeckte Auswirkung auf das Endergebnis haben kann - Veränderungen sind bemerkbar.

Elektronisch repräsentierte Stimmen sind nicht fixiert, sie lassen sich ohne jeglichen Nachweis verändern oder löschen. Erneute Auszählungen werden in einer undurchsichtigen der Öffentlichkeit verschlossenen Umgebung (einer Blackbox) durchgeführt. Ob die Stimme auf dem Stimmzettel der tatsächlichen Intention des Wählers entspricht ist fraglich, da der elektronische Stimmzettel manipuliert werden hätte können.[73]

Ein entscheidendes Kriterium für den Einsatz von Papierbelegen ist allerdings die Einhaltung der Wahlgrundsätze wie dem des Wahlgeheimnisses. So darf sich ein Papierbeleg nachträglich nicht einer Person zuordnen lassen, was etwa durch Seriennummern oder Zeitstempel auf den Belegen möglich wäre. VVPT können durch zusätzliche Transparenz und Sicherheit somit auch das Vertrauen der Bürger in das elektronische System steigern [OoBe04].

In dem ACM Policy Statement [ACM04] wird ebenfalls eine physikalische Kopie der Stimmabgabe empfohlen, die eine von den Wahlmaschinen unabhängige Überprüfung des Wahlergebnisses gewährleistet. Ein Gesetzesentwurf, der sogenannte „Holt-Bill" [Holt07], zur Verbesserung des *Help America Vote Act* von 2002 schlägt ebenfalls Papierbelege vor, um in Zweifelsfällen eine Nachzählung zu ermöglichen.

Es gibt bereits einige Hersteller von E-Voting-Maschinen, wie etwa Avante oder Populex, die Papierbelege in ihre E-Voting-Systeme integriert haben.

Das *Technical Guidelines Development Committee* (TGDC) der *U.S. Elections Assistance Commission* (EAC) hat bereits eine Resolution verabschiedet, nach der keine neuen Wahlmaschinen

[73] William Gazecki drehte zu diesem Thema einen Dokumentarfilm „Invisible Ballots" (2004) [Film2].

mehr zugelassen werden dürfen, die keine Papierbelege verwenden und somit keine unabhängige Überprüfung ermöglichen. Die Resolution bezieht sich allerdings nur auf neue Zulassungen, nicht auf bereits zugelassene Geräte.

Der Voter-Verified Paper Trail wird oft mit dem *Voter-Verified Paper Ballot* VVPB verwechselt. Beim Voter-Verified Paper Ballot dient der Papierstimmzettel als amtlicher Nachweis der Stimme, elektronische Geräte (etwa Scanner) werden lediglich eingesetzt, um schneller zu einem Ergebnis zu gelangen. Das Ergebnis der manuellen Auszählung gilt als rechtlich gültig. Beim Voter-Verified Paper Trail dienen die Papierbelege eher als Backup-Mechanismus für nachträgliche erneute Auszählungen, das amtliche Ergebnis geht aber aus der elektronischen Zählung hervor.

Voter-Verified Paper Trail Verfahren werden oft kritisiert, da sie versuchen Transparenz in einen von Natur aus nicht transparenten Prozess zu bringen. Daher ist der Einsatz von VVPT, besonders bei nachträglicher Installation in einem bereits eingesetzten E-Voting-System, umstritten. Zudem kann der VVPT das geheime Wahlrecht untergraben. Weitere Kritikpunkte sind, dass durch den Einsatz von VVPT nur zu höherer Komplexität und zu zusätzlichen Kosten kommen würde [Cast07].

Sarah Everett schrieb ihre Dissertation [Ever07] über eine Usability-Studie, bei der sie in ein selbst gebautes E-Voting-System beabsichtigte Fehler in den Bestätigungs-Screen vor dem endgültigen Abschicken einbaute, um zu sehen, wie die Benutzer des Systems darauf reagieren. Etwa zwei Drittel der Testpersonen bemerkten die Fehler nicht und schickten ihre Stimme so ab. Somit wurde gezeigt, dass Review-Screens am Ende der Stimmabgabe nicht effektiv genug sind, zudem noch ein kleiner Prozentsatz der Testpersonen (6 %) die Stimmabgabe als abgeschlossen betrachteten und das Gerät verließen, ohne die Stimme endgültig abzuschicken. Die Folgerung ist, dass selbst Papierausdrucke der Stimmen, die durch das E-Voting-System ausgegeben werden, von Wählern nicht nochmals überprüft werden würden.

Das Gegenteil zu VVPT und VVPB heißt *Hand-Counted Paper Ballot* HCPB, der der gängigen Stimmabgabe mit Papierstimmzettel und Urne gleich kommt und bei dem keine elektronischen Verfahren verwendet werden. Hier sei das Transparenzgebot wie auch das Öffentlichkeitsprinzip gewährleistet.

6.7.2 End-to-End Systeme und Bulletin Boards

*End-to-End System*e sind zusätzliche Hilfsmittel einer Wahl, bei denen Wähler die korrekte Speicherung ihrer Stimme überprüfen können, ohne das Wahlgeheimnis anderer Wähler zu verletzen. Die Überprüfung der eigenen Stimme wird so zu einem Teil eines Audit-Verfahrens, zu dem auch eine wiederholbare erneute Auszählung der Stimmen oder Überprüfbarkeit der Stimmabgabe gehören.

End-to-End Systeme (Beispiel eines Systems siehe Abbildung 22) bieten eine Möglichkeit, die durch die Einführung elektronischer Wahlverfahren verloren gegangene Transparenz dadurch zu verbessern, dass jeder Wähler die Möglichkeit hat, sich von der korrekten Stimmerfassung und -zählung selbst zu überzeugen. Somit wird auch das Vertrauen der Wähler in die Korrektheit des Wahlprozesses gesteigert.

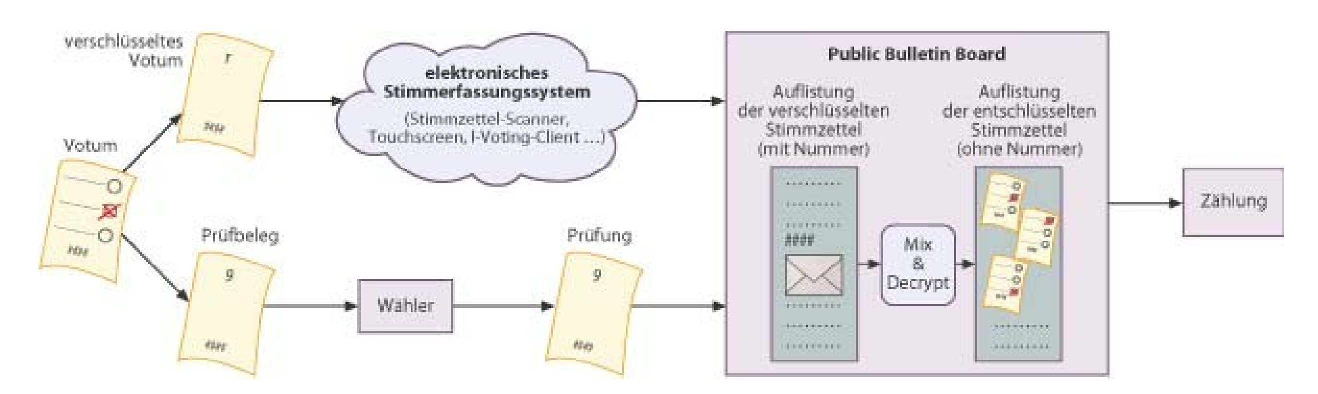


Abbildung 22: Grundprinzip von End-to-End Systemen. Quelle: [Siet07]

Die Basis eines End-to-End Systems ist ein für alle Wähler zugängliches *Bulletin Board*, das zur Verifikation der eigenen Stimme dient. Der Wähler erhält einen Beleg mit einer Nummer oder einer anderen Art eines eindeutigen Tokens, mit der er oder sie die abgegebene Stimme über das Bulletin Board überprüfen kann. Wichtig dabei ist, dass sich die Wahlentscheidung nicht mehr mit der Person des Wählers in Verbindung bringen lässt und der Beleg auch nicht als Beweis für Stimmenkäufer oder Erpresser gelten kann.

In den 1980er Jahren wurde dieses Konzept bereits von Cohen und Fischer [CoFi85] und von Josh Benaloh in seiner Dissertation vorgeschlagen [Bena87], später wurde es erweitert [BeTu94] und von einigen, vor allem jüngeren E-Voting-Schemas wieder neu aufgefasst und weiterentwickelt [Acqu04, AdRi06, ArFo08, BaFo01, BoGo02, CaGr05, ChHo05, ClCh08, DePe08, JuCa02, KiKo06, LeBo04, Neff04, StDu05, WaLe04, WaLe05].

6.7.2.1 Das SureVote System

David Chaum entwickelte hierzu ein Verschlüsselungsverfahren für Papierbelege, die nicht nur jeden Wähler überprüfen lässt, ob seine Stimme akkurat gesendet wurde, sondern auch dass diese richtig ins Wahlergebnis aufgenommen wurde [Chau04].

Bei dem daraus entstandenen kommerziellen Wahlverfahren *SureVote* wird die Stimme bereits vom Benutzer verschlüsselt an das Internetwahlsystem übergeben. Für jeden Wähler wird jede Möglichkeit der Stimmabgabe (etwa die möglichen wählbaren Parteien) auf einem anonymen, mit einer

Seriennummer versehenen Papierzettel kodiert übergeben. Die Stimme wird somit mit einem Code an ein E-Voting-System beliebigen Typs übergeben (siehe Abbildung 23) und mit einem Bestätigungscode, der mit dem auf dem Papierzettel übereinstimmen muss, bestätigt. So wird eine Art sicherer Kanal erreicht.

Ballot #:78694

Vote Code: 8991 Sure Code: 8753	Vote Code: 4197 Sure Code: 9779	SUBMIT
President and Vice President of the United States	United States Representative (Congress) District #16	State Senate District #35
George W. Bush & Dick Cheney (Republican)	Mark Foley (Republican)	David Vaughan (Republican)
Pat Buchanan & Ezola Foster (Reform)	Jean Elliot Brown (Democratic)	Tom Rossin (Democratic)
Al Gore & Joe Liberman (Democratic)	John McGuire (Reform)	Sherree Lowe (Reform)
David McReynolds & Mary Cal Hollis (Socialist)	You may vote the offices in any order. To vote a candidate for an office, enter the corresponding four-digit vote code shown on your ballot, press submit or the Return key, and then verify that the resulting sure code displayed matches that printed.	
Harry Browne & Art Oliver (Libertarian)		
Howard Phillips & J. Curtis Frazier (Constitution)		
Ralph Nader & Winona LaDuke (Green)		
Monica Morehead & Gloria La Riva (Workers World)		
James Harris & Margret Trowe (Socialist Workers)		
John Hagelin & Nat Goldhaber (Natural Law)		

Abbildung 23: Beispiel eines Stimmzettels beim SureVote Verfahren einer Testwahl auf www.surevote.-com

Das Verfahren CodeVoting [JoRi08], wie auch das *W-Voting* Wahlverfahren[74] der Wroclaw University of Technology [KlKu05], ist eine Weiterentwicklung des auch *Visual Voting* genannten Verfahrens von David Chaum.

[74] http://e-voting.im.pwr.wroc.pl

6.7.2.2 Das ThreeBallot System

Ronald Rivest stellte 2006 das Audit-Verfahren *ThreeBallot* [Rive06] vor, bei dem der Stimmzettel (bei einem Mehrheitswahlsystem) verdreifacht wird. Auf zwei Stimmzetteln wird für den Wunschkandidaten gestimmt und auf genau einem der drei gegen den Kandidaten (siehe Abbildung 24). Der Wähler kann nun eine Kopie jedes beliebigen der drei Stimmzettel machen, bevor alle drei Stimmzettel in die Wahlurne eingeworfen werden.

BALLOT		BALLOT		BALLOT	
President		President		President	
Alex Jones	○	Alex Jones	○	Alex Jones	○
Bob Smith	○	Bob Smith	○	Bob Smith	○
Carol Wu	○	Carol Wu	○	Carol Wu	○
Senator		Senator		Senator	
Dave Yip	○	Dave Yip	○	Dave Yip	○
Ed Zinn	○	Ed Zinn	○	Ed Zinn	○
3147524		7523416		5530219	

Abbildung 24: ThreeBallot Stimmzettel mit Seriennummern, Quelle Wikipedia http://en.wikipedia.org/wiki/ThreeBallot

Am Ende der Wahl werden die Stimmen auf einem anonymen Bulletin Board veröffentlicht, wobei der Wähler mit der Seriennummer auf dem kopierten Stimmzettel nachsehen kann, ob dieser im Gesamtergebnis enthalten ist.

Die Möglichkeit für Stimmenkauf ist nicht gegeben, da der Wähler einen beliebigen der drei Stimmzettel kopieren kann. Wurde ein Abschnitt gefälscht, wird dieser Schwindel mit einer hohen Wahrscheinlichkeit von einem Drittel durch den Wähler entdeckt.

Dieses End-to-End Audit-Verfahren kann auch nur auf Papier und ohne Computerunterstützung angewendet werden und zeigt eine mögliche Verschlüsselung der Stimme ohne Kryptografie, allerdings stellt dieses Verfahren eher eine akademische Übung dar, da seine Angriffspunkte weit kritisiert wurden und sich das System nach einem Pilotversuch mit Studenten am MIT als zu verwirrend herausstellte.

Einige kritische Arbeiten zum ThreeBallot Wahlverfahrens [Appe06, TjPe07] wurden wie auch einige Abwandlungen des Verfahrens [DePe08] nach der Entwicklung dieses End-to-End Systems veröffentlicht.

Bei Ronald L. Rivests *Scratch & Vote* [AdRi06] und Peter Ryans *Prêt à Voter* Schema [BrLi06, ChRy05] wird die gesamte Liste der Kandidaten bzw. Parteien in einer zufälligen Reihenfolge dargestellt (siehe auch Kapitel 4.4.2). Mit dem Abschnitt kann der Wähler ebenfalls die abgegebene Stimme auf einem Web-Bulletin Board überprüfen.

David Chaums *Scantegrity*[75] verwendet ein ähnliches Verfahren, bei dem jeder Stimmzettel mit einer eindeutigen Nummer und jedes Kästchen für eine Partei mit einem zufälligen Buchstaben versehen wird. Diese Kombination wird in einer separaten Datenbank ohne Hinweis zum Wähler gespeichert.

Die abgegebene Stimme (mit der individuell zugeordneten Buchstabenkombination zur Parteienliste) ist mit der Seriennummer auf einem öffentlichen Bulletin Board anonym vom Wähler nach der Entschlüsselung überprüfbar.

Der Nachteil dieses Verfahrens sind fortlaufende Seriennummern, die durch ein Beobachten der Ankunft der Wähler im Wahllokal eine Zuordnung zwischen Wähler und Stimmzettel möglich machen und somit das geheime Wahlrecht kompromittieren.

6.7.2.3 Die Punchscan Methode

Eine weitere Alternative ist die von David Chaum vorgestellte Punchscan-Methode[76], die ein Hybrid von Papier- und elektronischem Verfahren ist [FiCa06]. Dieses Verfahren basiert auf der Idee eines Voter Verified Paper Trail, also eines Papierbelegs für den Wähler, den er mitnehmen kann und mit dem er zu Hause seine Stimme nochmals überprüfen kann (siehe auch Kapitel 6.7.1). Der Papierstimmzettel besteht aus zwei Teilen: Eine obere Auflage, die die Kandidaten bzw. Parteien beschreibt, mit kleinen Löchern als Stimmfeld, und einen unteren Teil, bei dem ein Synonym für Kandidaten (a, b, c, etc.) steht. Die beiden Scheine werden übereinander platziert und mit einem breiten Filzstift wird ein Kandidat angekreuzt, wobei die Stimme auf beiden Scheinen markiert wird.

Der untere Teil des Wahlscheins stellt eine verschlüsselte Darstellung (Permutation) der Kandidatenliste dar, da beim Ausstellen des Wahlscheins die Anordnung der Kandidaten zufällig erzeugt wird. Mit einer Seriennummer werden die Stimmzettel den Wähler zugeordnet, die somit unterschiedliche Anordnungen der Kandidaten auf den Wahlscheinen vorfinden.

Folgende Schritte umfasst das Verfahren (Abbildung 25):

---

[75] http://www.scantegrity.org

[76] http://punchscan.org

  - *Pre-Election Audit*: Die Wahlkommission erzeugt die Stimmzettel und lässt sie von den Kandidaten überprüfen.
- Polling-Place Voting
  - *Mark in Booth:* Beide Seiten des Stimmzettels werden mit einem Stift markiert.
  - *Shred:* Der obere Stimmzettel mit der Beschreibung der Kandidaten wird vernichtet.
  - *Scan, Check, Cast:* Der untere Teil des Stimmzettels wird eingescannt und nach einer nochmaligen Überprüfung durch den Wähler übermittelt.
- *Post-Election Audit:* Über die Seriennummer der eingescannten Stimmzettel wird der Wähler und die Kandidatenliste ermittelt und die richtige Zuordnung als Stimme gespeichert.
  - Verifying at Home: Zu Hause kann der Wähler mit der Seriennummer seiner Wahl-Quittung überprüfen, ob seine Stimme in der öffentlichen Liste der Wahlergebnisse korrekt enthalten ist.

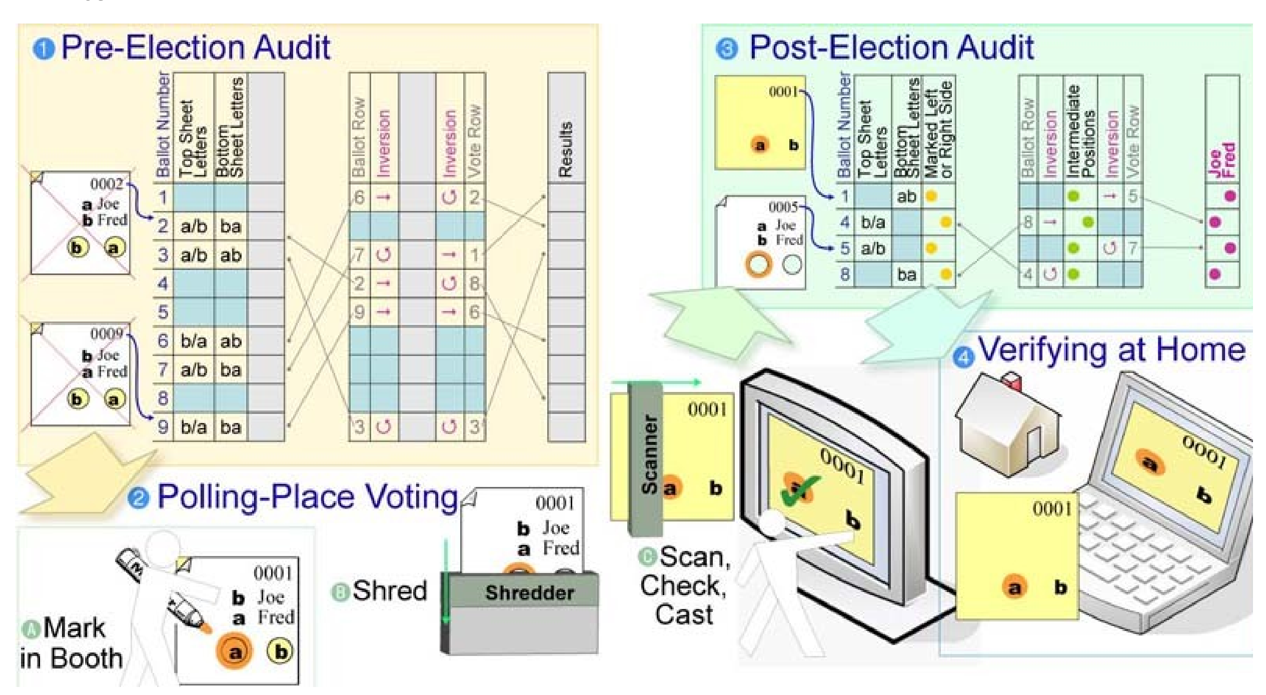


Abbildung 25: Ablauf des Punchscan-Verfahrens, Quelle http://punchscan.org

Nachteile des Systems sind die Bedienbarkeit für körperlich Behinderte, wie etwa Personen mit Sehschwächen. Weiters hat dieses System dieselben Nachteile, die das Lochkarten-System mit sich bringt (Undervote, Overvote), da die Stimmzettel mit optischen Scannern eingelesen und danach weiterverarbeitet werden.

Ein Sicherheitsrisiko besteht auch mit dem Shreddern der Stimmzettel als Methode zum Unkenntlichmachen der Stimmzettel. Im Demo wird ein horizontales Shreddern gezeigt, allerdings ist

ein derartiges Verfahren nicht angemessen für Aktenvernichtung, da die Felder für Stimmen direkt übereinander stehen und somit ein Streifen eine Reihe von Stimmen enthält.

Eine Kombination aus Punchscan und Prêt à Voter (siehe Kapitel 4.4.2 und 6.6.2) wurde ebenfalls vorgeschlagen [Lund08].

6.7.2.4 Probleme von End-to-End Systemen

Generell werden End-to-End Systeme häufig kritisiert, da vorgeworfen wird, dass dem bestehenden nicht transparenten und daher nicht vertrauenswürdigen Prozess ein zusätzliches meist noch komplexeres Verfahren hinzugefügt wird, durch das der Prozess der Stimmabgabe transparenter gemacht werden soll. Dies scheint aber der falsche Ansatz zu sein, da durch diese zusätzlichen Methoden der Kernprozess nicht verbessert werden könne. Fraglich bleibt somit, ob End-to-End Systeme das Vertrauen in E-Voting-Systeme tatsächlich steigern können, zudem diese Verfahren ebenfalls zusätzliche Manipulationsmöglichkeiten bieten (ist die Stimme, die auf dem Bulletin-Board gezeigt wird, auch die, die im Gesamtergebnis gespeichert wurde?) und den inhärent undurchsichtigen Prozess nicht verbessern können.

Bulletin Boards ermöglichen zudem einen nachträglichen Beweis der abgegebenen Stimme und eröffnen somit die Möglichkeit für Stimmenkäufe. Im konventionellen Wahlverfahren (siehe auch Kapitel 2.2) ist ein derartiges nachträgliches Audit-Verfahren nicht notwendig, da das Vertrauen in den Prozess gegeben ist.

6.8 Richtlinien und Normen

Eine Reihe von Richtlinien für die Sicherheit von IT-Systemen wurden im Laufe der Zeit herausgegeben. Hier folgt ein kurzer Auszug aus Österreich-relevanten Schriften, wie den OECD Richtlinien (siehe Kapitel 6.8.1), dem Österreichischen IT-Sicherheitshandbuch (siehe Kapitel 6.8.2), den ÖNormen (siehe Kapitel 6.8.3), den Empfehlungen des Europarates (siehe Kapitel 6.8.4) und dem IT-Grundschutz des Bundesamt für Sicherheit in der Informationstechnik (Kapitel 6.8.5).

6.8.1 OECD Richtlinien für die Sicherheit von Informationssystemen und -netzen

Die *OECD Richtlinien* (bzw. auch *Leitlinien* genannt) schlagen einen generellen Ansatz vor, bei dem bei allen Beteiligten (etwa den Mitarbeitern eines Unternehmens) ein Sicherheitsbewusstsein geschaffen werden soll. Diese Richtlinien sollen „die Entwicklung einer Sicherheitskultur fördern“.

Folgende neuen Grundsätze werden vorgeschlagen [OECD02]:

- Bewusstsein: Die Beteiligten sollten sich der Notwendigkeit der Sicherheit von Informationssystemen und -netzen und ihres Beitrages zur Erhöhung der Sicherheit bewusst sein.
- Verantwortung: Alle Beteiligten sind für die Sicherheit von Informationssystemen und -netzen verantwortlich.
- Reaktion: Die Beteiligten sollten rechtzeitig und in einer kooperativen Art und Weise handeln, um Zwischenfälle, die die Sicherheit gefährden, zu verhindern, aufzudecken und darauf zu reagieren.
- Moral: Die Beteiligten sollten die legitimen Interessen anderer respektieren.
- Demokratie: Die Sicherheit von Informationssystemen und -netzen sollte mit den wesentlichen Werten einer demokratischen Gesellschaft vereinbar sein.
- Risikoeinschätzung: Die Beteiligten sollten Risikoeinschätzungen durchführen.
- Sicherheitsgestaltung und -umsetzung: Die Beteiligten sollten Sicherheit als wesentlichen Bestandteil von Informationssystemen und -netzen aufnehmen.
- Sicherheitsmanagement: Die Beteiligten sollten ein umfassendes Sicherheitsmanagement-Konzept entwickeln.
- Neufestlegung: Die Beteiligten sollten die Sicherheit von Informationssystemen und -netzen überprüfen und neu festlegen und Sicherheitsstrategien, -praktiken, -maßnahmen und -methoden entsprechend ändern.

Diese Richtlinien richten sich an alle Beteiligten - an Regierungen, die Wirtschaft und Private - und bieten einen generellen Ansatz zum Schutz vor Angriffen durch ein geschaffenes Sicherheitsbewusstsein. Auf technische Details wird nicht eingegangen.

6.8.2 Österreichisches IT-Sicherheitshandbuch

Das österreichische IT-Sicherheitshandbuch [Stab02] besteht aus zwei Teilen. Zum einen beinhaltet es, wie die OECD Leitlinien, Grundlagen eines IT-Sicherheitsmanagement und weitere organisatorische Sicherheitsvorkehrungen, zum anderen werden technische IT-Sicherheitsmaßnahmen beschrieben.

Die Sicherheitsrichtlinien betreffen allerdings nur (Ausfall-)Sicherheit und Schutz - im Sinne von Safety - und befassen sich nicht mit (Angriffs-)Sicherung - im Sinne von Security.

6.8.3 Normen

In die Österreichischen Normen (ÖNORMEN) des Österreichisches Normungsinstituts werden teilweise Europäische Normen (EN) und Internationale Normen (wie ISO[77] oder IEC[78]) aufgenommen. Diese umfassen auch einen großen Bereich der IT-Sicherheit. Eine Reihe von Normen betreffen auch die Sicherheit von E-Voting-Systemen (siehe Tabelle 6).

Kürzel	*Beschreibung*
ISO/IEC 7816	Identification cards - Integrated circuit(s) cards with contacts
ISO 8372	Information processing - Modes of operation for a 64-bit block cipher algorithm
ISO/IEC 9796	Information technology - Security techniques - Digital signature scheme giving message recovery
ISO/IEC 9797	Information technology - Security techniques - Message Authentication Codes (MACs)
ISO/IEC 9798	Information technology - Security techniques - Entity authentication
ISO/IEC 9979	Data cryptographic techniques - Procedures for the registration of cryptographic algorithms
ISO/IEC 10118	Information technology - Security techniques - Hash functions
ISO/IEC 10536	Identification cards - Contactless integrated circuit(s) cards - Closecoupled cards
ISO/IEC 11770	Information technology - Security Techniques - Key Management
ISO/IEC TR 13335	Information technology - Guidelines for the management of IT Security
ISO 13491	Secure Cryptographic devices
ISO/IEC 13888	Information technology - Security techniques - Non-repudiation
ISO/IEC 14443	Identification cards - Contactless integrated circuit(s) cards - Proximitycards
ISO/IEC 14516	Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services
ISO/IEC 14888	Information technology - Security techniques - Digital signatures with appendix
ISO/IEC 15292	Information technology - Security techniques - Protection Profile registration procedures
ISO/IEC 15408	Information technology - Security techniques - Evaluation criteria for IT security
ISO/IEC TR 15443	Information technology - Security techniques - A framework for IT security assurance

[77] Internationale Organisation für Normung.

[78] International Electrotechnical Commission.

Kürzel	*Beschreibung*
ISO/IEC 15446	Information technology - Security techniques - Guide on the production of Protection Profiles and Security Targets
ISO/IEC 15693	Identification cards - Contactless integrated circuit(s) cards - Vicinity Integrated Circuit(s) Card
ISO/IEC 15816	Information technology - Security techniques - Security Information Objects
ISO/IEC 15945	Information technology - Security techniques - Specification of TTP services to support the application of digital signatures
ISO/IEC 18014	Information technology - Security techniques - Time stamping services
ISO/IEC 18033	Information technology - Security techniques - Encryption algorithms
BSI 7799 (Part 1) /ISO 17799	Information technology - Code of practice for information security management
BSI 7799 (Part 2)	Information Security Management Systems

Tabelle 6: Normen für die Sicherheit von E-Voting-Systemen [Stab02, Teil 2, Anhang A, S. 241ff]

Einige dieser Normen betreffen organisatorische Aspekte wie etwa die Norm BSI 7799 *Information Security Management*, die, ähnlich zum *CISSP Common Body of Knowledge* [MeHa07], den Aufbau eines IT-Sicherheitsmanagements und seiner Verankerung in der Organisation beschreibt. Andere Normen gehen sehr auf technische Details ein, wie die Beschreibung der Hash-Funktionen in Norm ISO/IEC 10118.

Die ÖNORMEN befassen sich im Wesentlichen mit (Bedrohungs-)Sicherheit - im Sinne von Security - vernetzter Systeme, aber nicht mit Safety oder Reliability. Außerdem umfassen die Normen kaum Sicherungsmaßnahmen für Hardware, noch menschliche Sicherheitsrisiken.

Parallel zu den ÖNORMEN gibt es noch die OVE[79] Bestimmungen und Normen, die in Kooperation des Verbands mit dem österreichischen Normungsinstitut entstanden sind und die ÖVE/ÖNORMEN, die Gerätesicherheit und -schutz umfassen.

6.8.4 Empfehlung des Europarates

Die Empfehlungen bzw. Standards des Europarates [CoE04] bestimmen die rechtlichen, operationalen und technischen Rahmenbedingungen für E-Voting-Systeme.

Die *rechtlichen Richtlinien* umfassen die Einhaltung der demokratischen Wahlrechtsgrundsätze (gleiche Wahl, freie Wahl, etc., siehe Kapitel 2.1) wie auch Transparenz, Verifizierbarkeit und Verantwortlichkeiten. Die *operationalen Richtlinien* betreffen den Ablauf vor, während und nach der

[79] Österreichischer Verband für Elektrotechnik.

Wahl und den Audit-Mechanismus. Die *technischen Empfehlungen* beinhalten Zugänglichkeit, Interoperabilität, Sicherheit und Zertifizierungen.

Die Empfehlungen bzw. Standards des Europarates decken viele Gebiete ab, beziehen Distanzwahlen neben Präsenzwahlen (vgl. Kapitel 1.4) ebenfalls mit ein, sind allerdings recht oberflächlich, gehen mehr in die Breite und nicht in die Tiefe.

Es wird oft auf Zuverlässigkeit und Sicherheit verwiesen, allerdings wird nicht auf Details eingegangen. So wird etwa gefordert, dass das E-Voting-System dem Wähler einen authentischen Stimmzettel präsentiert, wie das aber genau bewerkstelligt werden soll, wird nicht näher definiert.

Die *Europäische Kommission für Demokratie durch Recht* (auch *Venedig-Kommission* genannt) ist eine Einrichtung des Europarates, die ebenfalls Leitlinien für den „Verhaltenskodex bei Wahlen" herausgebracht [Vene02], in denen auf die Sicherheitsrisiken durch Angriffe auf mechanische oder elektronische Wahlen und auf notwendige Transparenz von E-Voting-Verfahren hingewiesen wird. Diese Leitlinien sind eher knapp gehalten, äußerst vage und dienen mehr der Übersicht.

6.8.5 BSI IT-Grundschutz

Die BSI-Standards für IT-Sicherheitsmanagement (100-1) [BSI05], für IT-Grundschutz-Vorgehensweise (100-2) [BSI05b], für Risikoanalyse auf der Basis von IT-Grundschutz (100-3) [BSI05c] und für Notfall-Management (100-4) [BSI08] bilden die vier Teile des IT-Grundschutzes nach dem deutschen *Bundesamt für Sicherheit in der Informationstechnik*.

Beim IT-Grundschutz wird ein recht weiter Ansatz gewählt. Hier wird versucht möglichst viele Bereiche abzudecken, wobei nicht zu sehr in die Tiefe gegangen wird. Im Wesentlichen wird auf anderen Standards wie ISO-Standard 2700, ISO 13335 und ISO 17799 aufgebaut.

6.9 Prüfverfahren und Zertifizierungen

Es gibt eine Reihe technischer Zertifizierungs- oder Prüfverfahren, die zur Überprüfung von sicherheitskritischen Systemen dient. Die Zertifizierung durch allgemein anerkannte Maßstäbe bietet die Möglichkeit zur Überprüfung, wie die getesteten Sicherheitssysteme tatsächlich funktionieren. Dadurch wird eine gewisse Transparenz erzeugt, die in weiterer Folge auch das Vertrauen und die Verlässlichkeit in neueste Technologien steigert. Einige dieser Zertifizierungen und Prüfverfahren werden hier vorgestellt.

6.9.1 Physikalisch-Technische Bundesanstalt

In Deutschland wurde die Physikalisch-Technische Bundesanstalt (PTB)[80] mit der Prüfung von Wahlmaschinen beauftragt. Es wurde geprüft, ob das Wahlgerät ESD1 nach den Bestimmungen der Bundeswahlgeräteverordnung (BWahlGV [BGBl99]) und des Wahlstatistikgesetzes (WStatG [BGBl02]) der Bundesrepublik geeignet ist, bei Bundestags- und Europawahlen zum Einsatz zu gelangen.

In dem Bericht der Prüfung eines Baumusters des Wahlgerät ESD1 des Herstellers Nedap wurde nach folgenden Kriterien geprüft:

I Prüfung der Bauarteigenschaften (diese Prüfung basiert auf dem BWahlGV[81], das die einzelnen Punkte für eine Prüfung vorgibt)

1 Identifizierung
2 Technischer Aufbau
 2.1 Konstruktion
 2.2 Belastbarkeit
 2.3 Haltbarkeit, Funktionssicherheit
 2.4 Rückwirkungsfreiheit
 2.5 Energieversorgung
 2.6 Transport und Aufbewahrung
3 Funktionsweise
 3.1 Funktionsprinzip, Verwendungsart
 3.2 Funktionskontrolle und Fehleranzeige
 3.3 Darstellung der Wahlvorschläge, Bedienungsvorrichtungen
 3.4 Stimmenspeicherung, Zählung und Anzeige [am ausführlichsten]
 3.5 Sperrung und Sicherung
 3.6 Abgabe von Stimmen
 3.7 Ergonomie, Bedienbarkeit
4 Bedienungsanleitung(en)

II Prüfung der Eigenschaften für eine repräsentative Wahlstatistik (diese Prüfung basiert auf dem WStatG[82], das die nötigen Eigenschaften vorgibt)

---

[80] Die Physikalisch-Technische Bundesanstalt in Deutschland entspricht in ihrer Tätigkeit dem Bundesamt für Eich- und Vermessungswesen (BEV) in Österreich, die somit mit der Prüfung von Wahlmaschinen beauftragt werden würde.

[81] BWahlGV - Bundeswahlgeräteverordnung: Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland.

Weiters zu beachten ist, dass nur ein einziges Baumuster überprüft und dass nur das Gerät und nicht der Wahlvorgang abseits der Wahlmaschine begutachtet worden ist. So wird etwa auch nicht auf Sicherheitsvorkehrungen im Umgang mit den Speichermodulen (EEPROMs[83]) nach dem Wahlvorgang eingegangen.

In den Prüfungsanforderungen des Berichts steht zwar, dass die Prüfung alle Sicherheitsaspekte umfassen solle, die an Wahlen gestellt werden, allerdings wurde bei den gewählten Prüfverfahren lediglich (Ausfall-)Sicherheit - im Sinne von Reliability - geprüft. So sind neben Security-Problemen (Schutz vor Angriffen etc.) etwa auch viele menschlichen Facetten (Risiko von Insidern, Art der Sicherung der Geräte zwischen den Wahlen, etc.) und Sicherheitsaspekte im Sinne von Safety außer acht gelassen worden.

Auf Basis der Prüfung des PTB hat der Deutsche Bundestag mit dem Beschluss zum Wahleinspruch 2006 [Bund05] folgende Stellungnahme gegeben: Die Manipulierbarkeit von Wahlcomputern ist zwar theoretisch gegeben, praktisch aber extrem unwahrscheinlich (betreffend den Austausch von Software auf den Geräten). Der Einspruch wurde mit folgender Begründung zurückgewiesen:

> „Die Wahlgeräte seien insbesondere hinreichend manipulationssicher und auch ein Papierprotokoll erhöhe die Manipulationssicherheit nicht. Auch eine Verletzung des Öffentlichkeitsgrundsatzes habe nicht vorgelegen.“ [Bund05, Abs. 35]

Dieser Beschluss des Bundestages basiert auf dem bestehenden Recht in Deutschland, das noch an moderne elektronische Wahlen angepasst werden muss. Die Bundeswahlgeräteverordnung BWahlGV aus dem Jahre 1975 (mit der letzten Änderung 1999) sieht (Manipulations-)Sicherheit generell nicht vor und widmet sich ausschließlich Sicherheit im Sinne von Reliability.

6.9.2 FEC-Standards

Die *Federal Election Commission* (FEC) der USA verfasste die *Voting System Standards* [FEC01], die von rund 80 % der Staaten der USA auf deren E-Voting-Maschinen angewendet werden. Die Standards wurden bereits überarbeitet und tragen daher den Titel „revised“.

Revised Performance Features: funktionelle und technische Fähigkeiten

[82] WStatG - Wahlstatistikgesetz: Gesetz über die allgemeine und die repräsentative Wahlstatistik bei der Wahl zum Deutschen Bundestag und bei der Wahl der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland.

[83] EPROM: Electrically Erasable Programmable Read Only Memory.

- Election Management Functions
- Feedback to Voter
- Accessibility
- Audit Trails
- Telecommunications
- Broadcasting of Unofficial Results

Revised Test Features: Tests unabhängiger Testbehörden

- Expanded Testing Standards
- Stages in the Test Process
- Distinction Between Initial Tests and Testing of Modifications to Previously Tested Systems
- Documentation Submitted by Vendors

Revised Organizational Features: Anpassung der Standards an verschiedene Benutzungsgruppen

- Multiple Volumes
- Standards, Guidelines and Fundamental System Development Techniques
- Inclusion of Selected Test Procedure Details

Issues Not Addressed by the Revised Standards: folgende Punkte werden nicht von den Standards erfasst

- Administrative Functions
- Integration with the Voter Registration Database
- Commercial Off-the-Shelf (COTS) Products
- Internet Voting
- Detailed Human Interface and Usability Standards
- Human Error Rate vs. System Error Rate

Das Verfahren deckt nicht alle Punkte der Sicherheit von E-Voting-Verfahren ab (Stichwort Human Factors) und schließt zudem auch spezifische Punkte explizit aus, wie die Überprüfung der eingesetzten kommerziellen Standard-Software (Commercial Off-the-Shelf (COTS) Produkte). Eine staatliche Regulierung oder gesetzliche Vorschrift, dass E-Voting-Systeme diesem Standard genügen müssen, gibt es nicht. Die Überprüfung wird zudem von unabhängigen Testbehörden durchgeführt, die allerdings von den Herstellern bezahlt werden.

Ein weiterer interessanter Aspekt der FEC-Standards ist, dass in den ursprünglichen Standards aus dem Jahre 1999 Papierbelege vorgesehen waren, aber in der überarbeiteten Version von 2002 nicht mehr vorkamen. Das Verschwinden der Empfehlung von Papierbelegen ist auf schlichtes Vergessen zurückzuführen, nicht auf Absicht (siehe auch Kapitel 6.7.1).

Einige der Staaten der USA haben bereits die freiwilligen Richtlinien der FEC, die einen Test- und Zertifizierungsprozess beinhalten, in ihre staatlichen Gesetze übernommen, allerdings gibt es kein nationales Gesetz, das einheitliche Richtlinien vorschreibt. Jedem US-amerikanischen Staat wird es selbst überlassen, Richtlinien und Gesetze zu verordnen [Jone01]. So kommt es dazu, dass einige amerikanische Staaten Papierbelege verwenden, andere wiederum keine vorsehen (siehe Abbildung 26). Eine Vereinheitlichung der Gesetze erweist sich allerdings als schwierig.

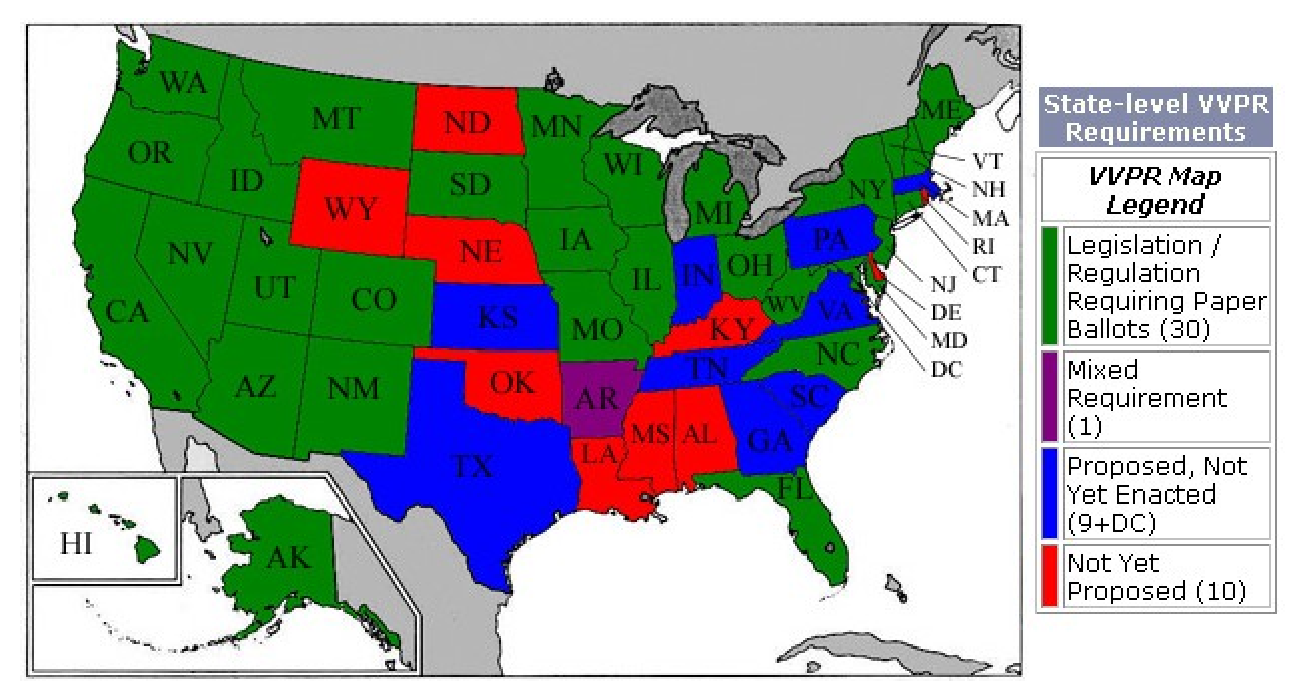


Abbildung 26: Verwendung von Voter Verified Paper Trail Verfahren in den USA, Quelle http://verifiedvoting.org

Die FEC-Standards werden häufig als zu wage, willkürlich und zu schwach bezeichnet. So scheinen etwa Werte für eine akzeptable Fehlerrate wie zufällig gewählt oder es werden etwa keine expliziten Attacken genannt, denen das getestete E-Voting-System standhalten soll [BaBi07].

Die Richtlinien von 2001 [FEC01] wurden 2002 überarbeitet [FEC02] und 2005 durch die *Voluntary Voting System Guidelines* (VVSG) [EAC05] der U.S. *Election Assistance Commission* (EAC) erweitert.

6.9.3 Common Criteria

Common Criteria[84] (zu Deutsch wörtlich „Gemeinsame Kriterien“, kurz CC) ist ein internationaler Standard für die Bewertung und Zertifizierung der Sicherheit von Computersystemen. Dieser Standard soll andere Zertifizierungen wie den europäischen ITSEC[85]- und den amerikanischen TCSEC[86]-Standard, auch bekannt als das *Orange Book*, ablösen.

CC ist in die Bewertung der Vertrauenswürdigkeit (Qualität der Methoden und Richtigkeit der Implementierung) und in die Bewertung der Funktionalität (Unterteilung in Funktionsklassen) gegliedert.

Es gibt sieben Evaluierungsstufen der Vertrauenswürdigkeit:

- EAL-1 funktionell getestet
- EAL-2 strukturell getestet
- EAL-3 methodisch getestet und überprüft
- EAL-4 methodisch entworfen, getestet und nachgeprüft
- EAL-5 semiformal entworfen und getestet
- EAL-6 semiformal verifizierter Entwurf und getestet
- EAL-7 formal verifizierter Entwurf und getestet

EAL-1 ist die niedrigste und EAL-7 die höchste Stufe der Vertrauenswürdigkeit. Das Sicherheitsniveau EAL-4 gilt als Ziel der Zertifizierungen für kommerzielle Produkte. EAL-5 wird selten erreicht, da bereits formale Entwuftsmethoden und Überprüfungen vorausgesetzt werden.

Funktionalitätsklassen: Im Gegensatz zu anderen Zertifizierungen (wie etwa dem ITSEC) sind die Funktionalitätsklassen nicht hierarchisch gegliedert.

- FAU Security Audit: Sicherheitsprotokollierung
- FCO Communikation: Kommunikation
- FCS Cryptographic Support: Kryptografische Unterstützung
- FDP User Data Protection: Schutz der Benutzerdaten
- FIA Identification And Authentication: Identifikation und Authentisierung
- FMT Security Management: Sicherheitsmanagement
- FPR Privacy: Privatsphäre

[84] Beschrieben wird Version 3.1, 2006.

[85] Information Technology Security Evaluation Criteria, 1991.

[86] Trusted Computer System Evaluation Criteria, DoD Standard 5200.28-STD, December 1985.

- FPT Protection Of The Target Of Evaluation Security Functionality: Schutz der Sicherheitsfunktionen
- FRU Resource Utilisation: Betriebsmittelnutzung
- FTA Target Of Evaluation Access: Schnittstellen
- FTP Trusted Path/Channels: vertrauenswürdiger Pfad/Kanal

Funktionalitätsanforderungen untergliedern sich in Klassen und diese wiederum in Familien.

Eine Klasse ist eine Gruppe von Familien, die eine gemeinsame Zielsetzung verfolgen. Eine Familie ist wiederum eine Gruppe von Komponenten, die Sicherheitsziele teilen, sich aber in Schwerpunkt oder Schärfe unterscheiden können. In einer Familie wird mindestens eine Komponente beschrieben, die Sicherheitsanforderungen an die konkrete Funktionalität charakterisiert. Die Bewertung der einzelnen Komponenten führt zu einer Einordnung in eine bestimmte Evaluierungsstufe für die Vertrauenswürdigkeit.

Protection Profiles (Schutzprofile) bestimmen den Schutzbedarf und die Sicherheitsziele für Produktklassen. Sie stellen die Bedrohungen den Anforderungen gegenüber und bieten anerkannte Lösungen auf angemessen abstrakter Ebene für Sicherheitsprobleme einer Produktgruppe. Produkte werden in Produktgruppen eingeteilt, wobei ein Produkt als ein Paket aus IT-Software, Firmware und / oder Hardware darstellt, das die Funktionalität für den Gebrauch oder die Einbindung in einer Vielzahl von Systemen bereitstellt.

CC betrifft den gesamten Entwicklungsprozess eines Computerprogrammes. Es dient als Leitfaden für die Entwicklung sicherheitskritischer Systeme, deren Bewertung und zur Auswahl von IT-Sicherheitsprodukten.

Ein Nachteil der Common Criteria Zertifizierung ist, dass der Hersteller das betroffene Produkt bei einer beliebigen Stelle zertifizieren lassen kann, die er selber wähl (vgl. TÜV Zertifizierungen). Dadurch kann eventuell eine Zertifizierungsstelle gewählt werden, die weniger streng prüft als andere Stellen. Auch Einflussnahmen durch Bestechung können somit begünstigt werden. Eine staatliche Zertifizierungsbehörde, die eine bestimmte Zertifizierung vergibt, würde eine vertrauenswürdigere Vergabe der Zertifikate gewährleisten [Ande01].

Zudem gibt es kein weltweites CC-Profil für E-Voting. Es besteht zwar bereits ein Schutzprofil für den Wahlstift [BSI07] (siehe auch Kapitel 6.10.2), an einem Schutzprofil für Internetwahlen wird derzeit bei der *Gesellschaft für Informatik* (GI) gearbeitet, ohne vollständige Ergebnisse. Basis für ein derartiges Schutzprofil ist der ISO Standard (ISO/IEC15408) für Information Technology Security Evaluation, allerdings ist die Anforderungen an das erarbeitete Profil, dass es Sicherheitsanforderungen von Vereinswahlen abdecken soll [GI07].

6.9.4 Andere Standards

Das *Institute of Electrical and Electronics Engineers* (IEEE) arbeitet seit 2001 an den *Voting Equipment Standards* im Rahmen des Projekts 1583. Der Standard soll elektronische, mechanische und menschliche Aspekte berücksichtigen und folgende Merkmale eines E-Voting-Systems sicherstellen: Barrierefreiheit (*Accessibility*), Genauigkeit (*Accuracy*), Vertraulichkeit (*Confidentiality*), Zuverlässigkeit (*Reliability*), Schutz (*Security*), Bedienbarkeit (*Usability*) [IEEE01].

Die Information Systems Security Association (ISSA) veröffentlichte in den 1990er Jahren die Generally-Accepted System Security Principles (GASSP), die generelle Richtlinien für die Einhaltung der Sicherheit bei Informationssystemen enthalten [Poor99]. Die GASSP betrifft, wie auch Common Criteria (siehe Kapitel 6.9.3), den gesamten Prozess der Entwicklung eines Systems.

6.10 Alternativen zu E-Voting

Es wurde eine Reihe von Alternativen zu gewöhnlichen E-Voting-Systemen wie DRE-Wahlsystemen entwickelt. In diesem Kapitel wird eine Übersicht über andere Möglichkeiten der elektronischen Unterstützung bei Wahlen gegeben.

6.10.1 Ballot-Marking Machine

Die *Ballot-Marking Machine* wurde von einigen Wissenschaftlern vorgeschlagen und ist eine Alternative zu DRE-Wahlsystemen. Dieser Typ von Wahlgeräten dient lediglich einer elektronischen Registrierung der Stimme und gibt Papierbelege aus. Aviel Rubin schlägt ein Touchscreen-Gerät vor, das ein standardisiertes Layout und standardisierte Typografie hat, mit dem der Stimmzettel elektronisch dargestellt und die Stimme auf dem Gerät abgegeben wird. Under- und Overvotes werden durch die Abgabe der Stimme über das Touchscreen-Gerät verhindert, ungültig Wählen ist weiterhin möglich. Das Gerät druckt Papierstimmzettel aus, die dann auch in eine Urne geworfen werden. Die Zählung ist somit unabhängig von dem Wahlsystem, da die Stimmzettel später per Hand oder mit optischen Scannern ausgezählt werden können. Aussagekräftige manuelle Neuzählungen sind durch die Papierbelege möglich. Zusätzlich sind optische Scanner mit Audio-Ausgabe angedacht, die Blinden den Stimmzettel „vorlesen“ können, damit auch beeinträchtigte Personen ihre Stimme verifizieren können.

Die Anforderungen an eine Ballot-Marking Machine sind Folgende [Rubi06, S. 207]:

- Transparenz: offener, nicht proprietärer Code
- Unabhängiger Audit: Wahlbeobachter, VVPB

- Peer Reviews
- Usability Testing

Rebecca Mercuri stellt eine Abwandlung dieses Systems mit ihrer *The Mercuri Method* vor. Ihr System hat ebenfalls ein Touchscreen zur Darstellung des Stimmzettels und zur Eingabe der Stimme mit Papierbelegen, allerdings bekommt der Wähler den Papierstimmzettel nicht in die Hand, sondern kann ihn hinter einer Glasscheibe nochmals überprüfen [Merc02] .

Diese Methoden schaffen mehr Transparenz in einem elektronischen Wahlsystem, allerdings sind diese Systeme mit den Nachteilen der Papierbelege behaftet (siehe auch Kapitel 6.7.1).

6.10.2 Digitales Wahlstift-System

Eine Alternative zu Lochkartensystemen und Touchscreen-Automaten bietet der sogenannte *Hamburger Wahlstift dotVote*. Der Hamburger Senat hat im Winter 2006 beschlossen, dass für die Bezirksversammlungs- und Bürgerschaftswahlen im Februar 2008 ein digitaler Stift eingesetzt werden solle. Dieser Stift ist ein Schreibgerät (siehe Abbildung 27), das eine kleine Kamera hinter der Kugelschreibermine enthält (vgl. digitaler Stift des Herstellers *Anoto*), die mit einer kaum sichtbaren Rasterung auf dem Stimmzettel die Kreuze mit der Mine erkennt und speichert.



Abbildung 27: Digitaler Wahlstift.
Quelle: http://dotVote.de

Das Gerät wird, bevor es an den Wähler ausgegeben wird, initialisiert. Die Stimme wird beim Ankreuzen des Papierstimmzettels zusätzlich auf dem Stift elektronisch gespeichert. Nach dem Abstimmen wird der Papierstimmzettel wie gewohnt in eine Urne geworfen und das Gerät wieder an die Wahlkommission zurückgegeben, die die Stimme von dem Stift mittels USB ausliest. Dieser Vorgang hat den Vorteil, relativ schnell ein Wahlergebnis präsentieren zu können, ohne auf die bewährten Stimmzettel verzichten zu müssen. Ein Kritikpunkt ist allerdings, dass nach den Anforderungen des Systems die digitale Stimme der Stimme auf dem Papierbeleg vorzuziehen ist.

Die Sicherheitsanforderungen des CC Schutzprofils [BSI07] wurden vom deutschen Bundesamt für *Sicherheit in der Informationstechnik* (BSI) zertifiziert [BSI07a] (siehe auch Kapitel 6.9.3). Für Oktober 2007 ist ein Einsatz des digitalen Stiftes in zehn „Schnupperwahllokalen“ (z. B. in Einkaufszentren) geplant.

Der Chaos Computer Club zeigte kurz nach Vorstellung des Wahlstiftes mögliche Attacken auf. So könne etwa mit einem „trojanischen“ Stift, der genauso aussieht, wie der Wahlstift selbst, beim Anschließen an die Auslesestation fremde bösartige Software auf das System übertragen werden. Zudem kam es zu einem demonstrativen Manipulationsversuch, wo die Schraffur auf dem Stimmzettel, das der Stift ausliest, manipuliert wurde. Mit diesem Hack wurde gezeigt, dass die Stimmen manipuliert werden können, da der Wähler so sein Kreuz bei einer Partei macht, aber die digitale Stimme zu einer anderen Partei gespeichert wird.

7 Methode zur Bewertung und Optimierung der Sicherheit von E-Voting-Systemen

Die hier vorgestellte *E-Voting-System Security Optimization* Methode, kurz EVSSO-Methode, zur Bewertung der Sicherheit[87] von E-Voting-Systemen ist durch die Analyse zahlreicher E-Voting-Systeme und deren Problemen und Sicherheitsmängel entstanden (siehe auch Kapitel 5 und Kapitel 6).

Die Methode ist ein Hilfsmittel zur Optimierung der Sicherheit (im Sinne von Safety und Security, siehe Kapitel 3.1) von E-Voting-Systemen (im Speziellen von DRE-Wahlsystemen), mit dem der Reifegrad der Sicherheit von E-Voting-Systemen objektiv und detailliert bestimmt werden kann. Durch den checklisten-artigen Aufbau der Richtlinien ermöglicht dieses Modell die Formulierung konkreter, in die Praxis umsetzbarer Vorschläge zur Optimierung der Safeguards des getesteten E-Voting-Systems.

Mit dieser Methode können verschiedene E-Voting-Systeme bewertet und dann miteinander verglichen werden. Dieser Ansatz bietet ein generisches Bewertungsschema und ist daher auf eine Reihe von E-Voting-Systemen (vor allem DRE-Wahlcomputer) anwendbar. Internetwahlverfahren werden durch diese Methode allerdings nicht abgedeckt, da I-Voting-Systeme als inhärent unsicher gelten (kein geheimes oder freies Wahlrecht, Wählerbeeinflussung, Stimmenkauf, Denial-of-Service Attacken, keine Möglichkeit eines authentischen Audit-Verfahrens, etc., siehe auch Kapitel 1.4) [BrJe01, DiSi08, IPI01, JeRu04a, MuVa98, Merc02, NeMe00, Phil02, Rubi02, Wein00].

Sicherheit zu bewerten ist generell ein schwieriges Unterfangen, da sich Sicherheit oft nur schwer quantifizieren lässt (vgl. Risikobewertung Kapitel 3.3.3). Es stellt sich oft als diffizil heraus, konkrete Verbesserungsvorschläge und Schritte für die Erhöhung der Sicherheit von E-Voting-Systemen zu bestimmen.

7.1 Ähnliche Arbeiten

Wissenschaftler der Universität Washington stellten ein Framework [SaPo06] vor, mit dem (theoretische) E-Voting-Schemata miteinander verglichen werden. Dabei werden mehrere Aspekte der Sicherheit (*Eligibility. Privacy. Verifiable. Dispute-free, Accuracy, Fair, Robust, Receipt-free, Incoercible, Scalable, Practical*) einer Reihe von E-Voting-Protokollen mit Hilfe von Venn-Diagrammen[88] miteinander verglichen. Eine Auswahl von E-Voting-Protokollen wird in drei große Kategorien einge-

[87] „Sicherheit" wird im Sinne von Security inklusive aller zusammenhängender Begriffe wie Systemstabilität, Vertraulichkeit, Integrität, Verfügbarkeit, Zuverlässigkeit, Safety und Wartbarkeit verwendet. Siehe auch Kapitel 3.1.1.

[88] Venn-Diagramme werden auch Mengendiagramm genannt.

teilt: Verdeckte Wähler, verdeckte Stimmen und verdeckte Wähler mit verdeckten Stimmen. Diese Arbeit bezieht sich auf theoretische Modelle und dient zum Vergleich dieser Schemata in Bezug auf deren Sicherheitseigenschaften.

In einer anderen Arbeit [Grit03] wurden ebenfalls E-Voting-Schemata nach verschiedenen Aspekten der Sicherheit (*Accuracy (Inalterability, Completeness, Soundness), Democracy (Eligibility, Unreusability), Privacy, Robustness, Verifiability, Uncoercibility, Fairness, Verifiable participation*) miteinander verglichen.

Beide Arbeiten befassen sich mit den theoretischen Grundlagen von Wahlen, setzten sich aber nicht mit der praktischen Anwendung oder komplexen E-Voting-Systemen (oder auch nur Teilen dessen: Software, Hardware oder Human Factors) auseinander.

Einige Standards für die Konstruktion und Zertifizierung von E-Voting-Systemen wurden entwickelt, wie die FEC-Standards oder das Common Criteria (siehe Kapitel 6.9), allerdings sind diese Standards nicht verpflichtend oder noch nicht ausgereift.

Weitere Bewertungsmodelle zur Analyse von Abläufen sind TPI und CMM, die in ihrer Methodik der vorgestellten Methode zur Bewertung der Sicherheit von E-Voting-Systemen ähneln.

Das *Test Process Improvement*-Modell (TPI®) [PoKo02] ist ein Modell zur Verbesserung der Qualität des Testprozesses im Softwareentwicklungsumfeld. Mit diesem Werkzeug können Verbesserungsvorschläge zur Optimierung des Testablaufes formuliert werden. Das *Capability Maturity Model©* (CMM) [Hump89] des *Software Engineering Institutes* (SEI) dient zur Aufbesserung des gesamten Softwareprozesses von der Softwareentwicklung bis zur Konfiguration und Wartung. *Capability Maturity Model Integration* CMMI® ist der Nachfolger des CMM [Kneu06].

Diese Modelle ähneln der Methodik der Bewertung mit der EVSSO-Methode, allerdings wird ein anderer Fokus - nämlich der Reifegrad des Softwaretest- bzw. Softwareentwicklungsprozesses - gewählt.

7.2 Kernbereiche der EVSSO-Methode

Die Methode ermöglicht die Beurteilung der Sicherheit bezüglich verschiedener Aspekte. Durch die Bewertung dieser Aspekte werden die Stärken und Schwächen von Sicherheitsmaßnahmen eindeutig festgestellt. Diese Aspekte werden *Kernbereiche* genannt.

Um Sicherheit bei E-Voting-Systemen zu gewährleisten, muss man einen ganzheitlichen Ansatz wählen, der alle Teile dieses komplexen Systems inklusive menschlicher Faktoren berücksichtigt. Wird nicht jedes Element des Systems auf dessen spezifische Sicherheitsmerkmale, auf Sicherheitsmerkmale der Schnittstellen zu anderen Komponenten und auf dessen Einfluss auf das gesam-

te System hin überprüft, kann die Sicherheit des gesamten Systems nicht gewährleistet werden. Dieser Ansatz wird auch *Holistic Security* (ganzheitliche Sicherheit) genannt [McLa05].

Somit müssen alle Teile eines Systems inklusive aller Facetten von Sicherheit, wie Safety und Security, Systemstabilität, Vertraulichkeit, Integrität, Verfügbarkeit, Zuverlässigkeit, Safety und Wartbarkeit, ebenfalls berücksichtigt werden (siehe auch Kapitel 3.1.3).

Ähnlich zur Unterteilung in physische, technische und organisatorische Sicherheit [Nagy05] (siehe auch Kapitel 3.5) und zur Unterteilung in physikalische, syntaktische und semantische Attacken [Schn00] (siehe auch Kapitel 5) wird mit dieser Methode zwischen folgenden drei Hauptbereichen eines E-Voting-Systems unterschieden: Hardware, Software und Human Factors (vgl. Unterteilung von Sommerville in Systemhardware, Systemsoftware und Menschlicher Bediener des Systems [Somm07, S. 73], siehe auch Kapitel 4.2).

Jeder dieser Hauptbereiche ist in weitere *Kernbereiche* untergliedert:

Bereich *Hardware*:

- Einhaltung der Wahlgrundsätze
- Safety
- Security
- Kryptografie

Bereich *Software*:

- Einhaltung der Wahlgrundsätze
- Datenintegrität
- Kryptografie
- Transparenz
- Softwareentwicklung
- Schutz der Software

Bereich *Human Factors*:

- Einhaltung der Wahlgrundsätze
- Sicherheitsmanagement
- Benutzerinterface
- Transparenz
- Gestaltung der Wahl

- Independent Testing Authority Validierung

Jeder Kernbereich umfasst eine Reihe von Kriterien, die einem speziellen Sicherheitsthema zugeordnet werden. Die Kriterien dieser Kernbereiche sind wiederum in Stufen eingeteilt (siehe auch Kapitel 7.3) und jeder Kernbereich des E-Voting-Systems wird einzeln bewertet.

7.2.1 Einhaltung der Wahlgrundsätze

In jedem der drei Hauptbereiche Hardware, Software und Human Factors gibt es jeweils einen Kernbereich „Einhaltung der Wahlgrundsätze“. Eine Anforderung an elektronische Wahlen ist, dass sie mindestens so sicher gestaltet sein müssen wie herkömmliche Wahlen (siehe auch Kapitel 2.2). Grundlegend für E-Voting-Systeme ist die Einhaltung der Wahlgrundsätze [Jone03a] (siehe Kapitel 2):

- Allgemeines Wahlrecht: Jeder darf wählen
- Freies Wahlrecht: Entscheidungsfreiheit (durch Darstellung des Stimmzettels)
- Gleichheit: ein Stimmzettel pro Wähler
- Unmittelbares Wahlrecht: Wählen ohne Wahlmänner
- Verhältniswahlrecht: Die Sitze werden proportional zum Ergebnis verteilt
- Geheimes Wahlrecht: Anonymität
- Persönliches Wahlrecht: Ohne Stellvertreter persönlich wählen (Handhabung für (seh-)behinderte Wähler)
- Öffentlichkeit und Transparenz

Wird nur einer dieser Wahlgrundsätze nicht eingehalten, ist das gesamte E-Voting-System als unbrauchbar einzustufen - das wird in der EVSSO-Matrix abgebildet, indem die Einhaltung der Wahlgrundsätze höchste Priorität hat (siehe Kapitel 7.4).

Die EVSSO-Methode basiert auf den rechtlichen Grundlagen von Wahlen in Österreich, lässt sich allerdings auf E-Voting-Systeme der meisten demokratischen Republiken anwenden, da im Wesentlichen die gleichen Wahlgrundsätze gelten.

7.3 Stufen der EVSSO-Methode

Jeder der 16 Kernbereiche wird je nach Erfüllung der Kriterien auf einer bestimmten Stufe nach der Bestimmung des Reifegrades der Sicherheit eingeordnet. Die Stufen sind dabei so definiert, dass

Verbesserungen von einer niedrigeren auf eine höhere Stufe einen deutlichen Einfluss auf die Qualität der Sicherheit haben. Die Kriterien für die Erreichung einer bestimmten Stufe pro Kernbereich werden weiter unten (siehe Tabelle 7) genauer definiert.

Es gibt jeweils drei Stufen (A, B und C), die pro Bereich genau definiert werden. Manche dieser Kriterien der Stufen sind sehr ausführlich und enthalten viele Punkte, die erfüllt werden müssen, um diese Stufe zu erreichen, manche Kriterien enthalten nur einige wichtige Punkte. Bei manchen Kernbereichen werden nur die Stufen A oder A und B definiert, bei manchen werden alle drei Stufen verwendet.

Alle Kernbereiche und Stufen werden miteinander in der *EVSSO-Matrix* (siehe Kapitel 7.4) in Verbindung gebracht, um Prioritäten und Abhängigkeiten zwischen den Kernbereichen und den Stufen darzustellen. In der EVSSO-Matrix werden die verschiedenen Stufen der Kernbereiche jeweils einer *Entwicklungsebene* zugeordnet. Daraus ergibt sich eine Matrix mit zehn Entwicklungsebenen des Sicherheitsreifegrades.

Die Einstufung der Kernbereiche ergibt die Reife bzw. die Qualität der Sicherheit des E-Voting-Systems. Jede höhere Stufe (C ist höher als B, B ist höher als A) ist besser (also sicherer) als die Stufe darunter. Indem Stufen verwendet werden, kann die aktuelle Sicherheitssituation des E-Voting-Systems genau bewertet werden. Es ermöglicht zudem das Erkennen schrittweiser Verbesserungen für die Sicherheit des bewerteten Systems.

Jede Stufe wird durch bestimmte Kriterien bzw. Anforderungen an den jeweiligen Kernbereich definiert. Werden diese Anforderungen (auch Kriterien genannt) erfüllt, ist die jeweilige Stufe erreicht. Für die Erlangung einer höheren Stufe wird die Erfüllung der Anforderungen der niedrigeren Stufen vorausgesetzt. So müssen, um Stufe B zu erreichen, neben den Anforderungen von Stufe B auch die Anforderungen von Stufe A erfüllt werden. Wenn Stufe C erfüllt wird, jedoch nicht Stufe B, so ist die Komponente in Stufe A einzuordnen. Wird Stufe A nicht erfüllt, hat dieser Kernbereich eine nicht definierte Stufe und wird auf Entwicklungsebene 0 eingeordnet.

Unterhalb (siehe Tabelle 7) werden die Anforderungen in Stichworten für die Stufen der Kernbereiche gegeben (eine ausführliche Liste ist im Anhang Appendix A angeführt):

Stufe *Kernbereiche*	*A*	*B*	*C*
1 Hardware - Einhaltung der Wahlgrundsätze	- Geheimes Wahlrecht: keine lineare / zeitliche Rückverfolgbarkeit zum Wähler - Geheimes Wahlrecht: Verwendung von Wahlkabinen	- Öffentlichkeit und Transparenz: Zugriff auf Geräte, Speichermedien und deren Dokumentation - Zugriff auf Geräte und Speichermedien beim Aufbau und beim Einsatz limitieren	- Lagerung, Sperrung und Versiegelung der Geräte und der Speichermedien, regelmäßige Überprüfung und Dokumentation der Sicherheitsvorkehrungen - Geheimes Wahlrecht: Schutz vor TEMPEST Attacken und Minimierung des Geräuschpegels
2 Hardware - Safety	- Korrektheit der Konstruktion - Homogene Architektur - Sicherheit der Konstruktion und Installation	- Belastbarkeit - Haltbarkeit, Funktionssicherheit - Schutz bei Transport und Aufbewahrung - Energieversorgung	- Notfallplan - Rückwirkungsfreiheit
3 Hardware - Security	- Schutz vor physikalischen Attacken - Keine Internetverbindung(-smöglickeit) - Entfernen nicht benutzter Geräte - Zutrittskontrolle zu Maschinen	- Schutz der Speichermedien: Physikalische Attacken, Entfernbarkeit der Module, Methoden um Kopien der Speichermedien zu erkennen	- Schutz vor (internen) Denial-of-Service Attacken, redundante Systeme - BIOS Passwörter setzen
4 Hardware - Kryptografie	- Verwendung sicherer, anonymer Verbindungen	- Hardware-Verschlüsselung der	

Stufe *Kernbereiche*	*A*	*B*	*C*
		Festplatten	
5 Software - Einhaltung der Wahlgrundsätze	- Allgemeines Wahlrecht: korrekte Erfassung der Wählerevidenz - Gleichheit: ein Stimmzettel pro Wähler, die Stimmen zählen gleich viel - Geheimes Wahlrecht: anonyme Kanäle, verschlüsselte Verbindungen, anonyme Stimmabgabe am Urnenserver	- Öffentlichkeit und Transparenz: Sourcecode durch Peer-Reviews analysieren, Nachvollziehbarkeit der Stimmabgabe - Öffentliche Liste der verwendeten zusätzlichen Software	- Öffentlichkeit und Transparenz: Sourcecode der Firmware, der Geräte-Treiber und der eingesetzten COTS[89] Produkte offenlegen
6 Software - Datenintegrität	- Korrektheit der Implementierung von Stimmenspeicherung, Zählung und Anzeige - Managementfunktionen und Audit-Funktionen der Wahlsoftware	- Schutz der Daten und Ausfallsicherheit: Datenverlust nach Absturz der Maschine (Backup Systeme) - Verwendung synchronisierter, interner Uhren der Maschinen	
7 Software - Kryptografie	- Vertrauenswürdiger Pfad / Kanal - Schutz der Benutzerdaten und des Stimmzettels - Einsatz asymmetrischer Schlüssel (Chipkarten) für Identifikation, Authentisierung und Autorisierung	- Einsatz von „starken" aktuellen Krypto-Algorithmen - Key Management - Methoden um Kopien und Manipulationen der Speichermedien zu erkennen	- Verschlüsselung von Konfigurationsfiles und Datenbank
8 Software - Transparenz	- Sourcecode der Wahlsoftware zur Überprüfung durch Dritte verfügbar machen, Peer-Reviews - Wiederholte Testwahlen vor der rechtskräftigen Wahl	- Test der COTS-Produkte, des Betriebssystems und des BIOS - Internes Fehleranalyse-System	

[89] COTS: Commercial Off-the-Shelf.

Stufe *Kernbereiche*	*A*	*B*	*C*
9 Software - Softwareentwicklung	- Qualitätsmanagement: Reviews in jeder Phase des Entwicklungsprozesses - Risikomanagement in der Planungsphase - Nachvollziehbarkeit, ob ein anonymer Stimmzettel abgegeben wurde - Überprüfung der Benutzereingaben - Interoperabilität mit bestehenden Systemen	- Qualitätsmanagement: automatische und manuelle Testbarkeit - Implementierungsrichtlinien - Security Tests und Auditing nach Implementierung: Blackbox Tests	- Teamaufteilung: duales Entwickeln - Security Tests und Auditing nach Implementierung: Review der Applikation auf Sicherheitsmerkmale, White Box Tests, Penetration Tests - Code Analysen (Metriken) - Interoperabilität für die Zukunft garantieren mit Verwendung offener, nicht proprietärer Standards
10 Software - Schutz der Software	- Homogene Betriebssysteme mit aktuellen Sicherheits-Updates - Keine Default-Passwörter oder PINs, „starke“ Passwörter	- Überprüfung der Version und der Integrität des Sourcecodes, der verwendeten externen (Standard-)Bibliotheken und der Konfigurationsdateien - Sicherheit des Update-Mechanismus - Nicht benötigte, vorinstallierte Software deinstallieren - Skalierbarkeit	- Überprüfung der Authentizität des Compilers - Schutz gegen diverse Software Sicherheitsrisiken wie Buffer Overflows, Viren, Würmern, Trojanern, Rootkits, etc. - Schutz vor Man-In-The-Middle Attacken
11 Human Factors - Einhaltung der Wahlgrundsätze	- Freies Wahlrecht: parteilose und neutrale Gestaltung des Stimmzettels und der Wahlmaschine. Es muss möglich sein, ungültig zu wählen	- Öffentlichkeit und Transparenz: Einsichtnahme einer Wahlkommission in Sourcecode und Zugang zu	

Stufe *Kernbereiche*	*A*	*B*	*C*
	- Persönliches Wahlrecht: Ohne Stellvertreter persönlich Wählen - Allgemeines Wahlrecht: Aufklärung und Einschulung der Wähler in das E-Voting-System	Wahlmaschinen	
12 Human Factors - Sicherheitsmanagement	- Einschulung des Personals und Erstellung von Sicherheitsplänen - Sicherheitsmaßnahme: duale Kontrolle - Protokollierung der Handhabung von Software, Hardware und Stimmspeichermedien zur lückenlos nachvollziehbaren Kontrolle aller Prozesse	- Hintergrund-Überprüfungen der Mitarbeiter - Security Awareness Trainings aller (externen) Mitarbeiter	
13 Human Factors - Benutzerinterface	- Darstellung des Stimmzettels auf einer Bildschirmseite, ohne Scrollen - Anordnung der Parteien muss dem Papierstimmzettel entsprechen - Adäquate Darstellung des Ablaufes der Stimmabgabe - Keine Wahlbeeinflussung - Korrekte Darstellung des Stimmzettels - Feedback während und nach Beendigung der Stimmabgabe - Online-Hilfe-Seiten bei jedem Schritt verfügbar - Akzeptable Antwortzeiten der Applikation	- Mehrsprachigkeit - Vergrößerungen (Lupe-Funktion) für Sehbehinderte - Audio-Unterstützung für Blinde, taktile Unterstützung	- Usabilityprüfung mit repräsentativer Testgruppe
14 Human Factors - Trans-	- Bereitstellung von Informationen rund um die Wahl	- Auditphase nach der Wahl mit Les-	- Ein öffentlich diskutierbares Wahl-

Stufe *Kernbereiche*	*A*	*B*	*C*
parenz	- Öffentliche Bekanntgabe der Bezirksergebnisse - Möglichkeit der Wahlbeobachtung, vor, während und nach der Wahl - Überprüfung, ob die Anzahl der abgegebenen Stimmen mit der Anzahl der Wähler übereinstimmt, die einen Stimmzettel angefordert haben - Anonyme Papierbelege (Voter Verified Paper Trail)	sons Learned für kommende Wahlen - Vergleich der Wahltagsbefragungen vom aktuellen und der vorangegan-genen Jahre - Bestimmung der Grenzwerte für manuelle Nachzählungen	protokoll und öffentlich verfügbare, „starke" kryptografische Algorithmen
15 Human Factors - Ge-staltung der Wahl	- Die Registrierung zur elektronischen Wahl soll kein Hin-dernis darstellen - Parallelbetrieb: alternatives Wählen mit Papierstimmzet-tel möglich - Zeitgleicher Beginn und Ende der elektronischen Stimm-abgabe mit den konventionellen Wahlen - Verzögerungen des Ablaufes der Stimmabgabe verhindern - Möglichkeit einer Teststimmabgabe	- Akzeptanz und Verbreitung (Kos-tenfaktor): Kostentragungspflicht für die Geräte bei öffentlichen Stellen	
16 Human Factors - Inde-pendent Testing Authority Validierung	- Überprüfung, Zertifizierung oder Test durch unabhängige Prüf-Anstalten (Independent Testing Authority (ITA)) auf Korrektheit und Sicherheit		

Tabelle 7: Beschreibung der Stufen der Kernbereiche

Durch die Definition dieser Stufen können Optimierungsmöglichkeiten vorgeschlagen werden. Erreicht ein Kernbereich eine gewisse Stufe, so ist eine Verbesserung der Sicherheit in diesem Bereich durch die Erlangung einer höheren Stufe des Kernbereichs möglich.

Zur Evaluierung eines E-Voting-Systems nach der EVSSO-Methode wird die ausführliche Checkliste (siehe Anhang Appendix A) verwendet, die alle Kriterien und Voraussetzungen für die Erfüllung einer Stufe eines Kernbereiches detailliert beschreibt. Jeder Punkt der Anforderungen wird überprüft und im Feld „OK“ markiert. Wird ein Kriterium nicht erfüllt, bietet die Spalte „Anmerkungen“ („Anm.“) die Möglichkeit eine Beschreibung für die Nichterfüllung einzutragen. So ist die Bewertung später auch für andere klar nachvollziehbar.

Die Checkliste wird als Basis für das Bestimmen der aktuell erreichten Stufen der Kernbereiche und für das Ausfüllen der EVSSO-Matrix verwendet.

7.4 Die EVSSO-Matrix

Nachdem für jeden Kernbereich die Stufe determiniert wurde, werden die Abhängigkeiten und Prioritäten der Stufen betrachtet. Nicht alle Stufen der Kernbereiche werden als gleich wichtig betrachtet. So ist zum Beispiel die Einhaltung der Wahlgrundsätze (Stufe A der Kernbereiche 1, 5 und 11) wichtiger als Stufe A des Kernbereichs 15. Diese Prioritäten können durch die EVSSO-Matrix abgebildet (siehe Tabelle 8) werden, indem die wichtigeren Stufen der Kernbereiche weiter rechts stehen, als die weniger hoch priorisierten.

Neben den jeweiligen Prioritäten gibt es ebenfalls Abhängigkeiten zwischen den einzelnen Kernbereichen. So machen etwa regelmäßige Integritätsprüfungen der Software (Stufe B von Kernbereich 10) erst nach einer generellen Qualitätssicherung (Stufe A von Kernbereich 9) Sinn. Die Abhängigkeiten werden in der EVSSO-Matrix verdeutlicht, indem die Erreichung einer Stufe für einen Kernbereich weiter rechts steht als die Stufe des Kernbereichs, der davon abhängig ist.

Diese Prioritäten und Abhängigkeiten werden durch die *EVSSO-Matrix* abgebildet. Die vertikale Achse listet die Kernbereiche auf, die Horizontale dient der Zuordnung der Stufen der jeweiligen Kernbereiche zu einer Entwicklungsebene. Die leeren Felder deuten auf den Abstand zwischen den Stufen hin, der überwunden werden muss, um eine Sicherheitsqualität eine Stufe höher zu erlangen. Eine Stufe zwischen den Feldern kann nicht erreicht werden. Erfüllt ein Kernbereich alle Kriterien der Stufe A und nur einige der Stufe B, wird er auf Stufe A eingestuft, bis er alle Kriterien für B oder C erfüllt. So bleibt ein Kernbereich solange mit Stufe A bewertet, bis er vollständig alle Kriterien der Stufe B erfüllt.

Entwicklungsebene *Kernbereich*	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
1 Hardware - Einhaltung der Wahlgrundsätze		A			B			C			
2 Hardware - Safety			A			B			C		
3 Hardware - Security			A			B				C	
4 Hardware - Kryptografie			A			B			C		
5 Software - Einhaltung der Wahlgrundsätze		A			B						C
6 Software - Datenintegrität			A			B					
7 Software - Kryptografie			A			B				C	
8 Software - Transparenz				A				B			
9 Software - Softwareentwicklung			A			B					C
10 Software - Schutz der Software				A					B		C
11 Human Factors - Einhaltung der Wahlgrundsätze		A			B						
12 Human Factors - Sicherheitsmanagement				A				B			
13 Human Factors - Benutzerinterface			A		B						C
14 Human Factors - Transparenz			A			B				C	
15 Human Factors - Gestaltung der Wahl					A			B			
16 Human Factors - ITA Validierung			A								

Tabelle 8: Die EVSSO-Matrix

Aus der EVSSO-Matrix lässt sich erkennen, dass etwa die Einhaltung der Wahlgrundsätze bei allen Hauptbereichen (Kernbereiche 1, 5 und 11) die höchste Priorität bei der Bewertung der Sicherheit eines E-Voting-Systems hat, da die Stufen A am weitesten links stehen. Das entspricht der Einhaltung der rechtlichen Grundlagen (siehe auch Kapitel 7.2.1).

7.5 Bewertung eines E-Voting-Systems mit der EVSSO-Methode

Die EVSSO-Matrix wird individuell für jedes E-Voting-System ausgefüllt, indem dieses in einem Assessment kritisch analysiert und für jeden Kernbereich der Status determiniert wird. Die erreichten Stufen werden in der EVSSO-Matrix grün, die nicht erreichten Stufen werden rot markiert und die Boxen zwischen den Stufen werden ebenfalls gefärbt. Wird bei einem Kernbereich Ebene A nicht erreicht, wird für diesen Kernbereich die Entwicklungsebene 0 grün gefärbt. Die Boxen zwischen einer erreichten Stufe und der darauf folgenden Stufe werden weiß gelassen, um den Abstand zwischen den Stufen visuell herauszuheben.

Zusätzlich wird zu jedem Kernbereich eine kurze Begründung angegeben, wieso eine gewisse Stufe erreicht wurde. So ist die Bewertung klar nachvollziehbar, auch für andere.

Ein fiktives Beispiel für eine, für ein spezielles E-Voting-System, ausgefüllte EVSSO-Matrix wird in Tabelle 9 gezeigt. In diesem Beispiel befindet sich etwa der Kernbereich 3 auf Stufe A, auch wenn möglicherweise bereits einzelne Punkte von Stufe C erfüllt sind.

Entwicklungsebene *Kernbereich*	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*Begründung*
1 Hardware - Einhaltung der Wahlgrundsätze		A			B			C				..
2 Hardware - Safety			A			B			C			..
3 Hardware - Security			A			B				C		..
4 Hardware - Kryptografie			A			B			C			..
5 Software - Einhaltung der Wahlgrundsätze		A			B						C	..
..												

Tabelle 9: Beispiel einer ausgefüllten EVSSO-Matrix nach einem Assessment eines E-Voting-Systems

Die Färbung der Matrix gibt ein deutliches Bild der Sicherheitsqualität des bewerteten E-Voting-Systems wider. Bereiche, die rot gefärbt sind, zeigen das Optimierungspotenzial des E-Voting-Systems in Bezug auf dessen Sicherheit, grüne Bereiche veranschaulichen den aktuellen Reifegrad der Sicherheit des Systems.

Aus der Matrix kann ebenfalls abgelesen werden, auf welcher Entwicklungsebene sich das System befindet, indem man die erreichten Stufen betrachtet. Es lässt sich erkennen, dass eine Entwicklungsebene erreicht ist, wenn die Spalte dieser Ebene nur grün oder weiß gefärbte Kästchen enthält. Aus der oben gezeigten Matrix eines beispielhaften E-Voting-Systems lässt sich erkennen, dass sich dieses System auf Ebene 1 befindet.

Die Entwicklungsebenen dienen allerdings nur als Hilfsmittel, keinesfalls als Maß für eine Gesamtbewertung der Sicherheit eines E-Voting-Systems. Sicherheit lässt sich schwer in Zahlen messen, deswegen wird auf eine Endnote in Form einer Zahl verzichtet. Eine klare Gesamtwertung lässt sich farblich kodiert aus der ausgefüllten EVSSO-Matrix nach einem Assessment eines E-Voting-Systems erkennen (viel Rot bedeutet etwa, dass es einen großen Optimierungsbedarf gibt, Ziel ist es die Matrix vollständig grün zu färben).

Optimierungsmaßnahmen lassen sich nun leicht aus der Bewertung ableiten: Wird eine Stufe nicht erreicht, lässt sich aus der Anforderungsliste der Stufe ersehen, welche Punkte nicht erfüllt werden konnten und welche Verbesserungen oder Erweiterungen somit notwendig sind, um die nächste Stufe zu erreichen.

Zudem ist auch eine Priorisierung der Optimierungsmaßnahmen eingängig, da die nächsthöheren Stufen angestrebt werden, die die Entwicklungsebene und damit die Gesamtbewertung des E-Vo-

ting-Systems erhöhen. Dies kann erreicht werden, indem auf die noch nicht erreichten roten Stufen, die am weitesten nach links reichen, hingearbeitet wird. In dem oben gezeigten Beispiel ist die Stufe A bei Kernbereich 4 zu priorisieren, da sich, wenn der Kernbereich Stufe A erreicht, die Gesamtbewertung schlagartig erhöht und das bewertete System Entwicklungsebene 3 erreicht. Ziel der Optimierungen ist, Entwicklungsebene 10 zu erreichen.

7.6 Analyse der EVSSO-Methode

Neben einer anschaulichen Visualisierung der Situation der Sicherheitsqualität und einer deutlichen Bewertung der Entwicklungsebene eines E-Voting-Systems, lassen sich auch mögliche schrittweise Optimierungspotenziale aus der EVSSO-Matrix klar ablesen. Der Hauptzweck der EVSSO-Matrix ist es die Stärken und Schwächen der Sicherheit des E-Voting-Systems aufzuzeigen und allen Beteiligten einen klaren Blick auf den aktuellen Sicherheitsstatus des Systems und dessen Verbesserungsmöglichkeiten zu geben. Die Anforderungen zur Erreichung bestimmter Stufen ergeben allgemein gehaltene Verbesserungsvorschläge, aus denen sich konkrete Maßnahmen ableiten lassen.

Die Verwendung dieses Modells allein garantiert jedoch noch keine gewünschte Verbesserung der Sicherheitssituation eines E-Voting-Systems, bietet aber ein Mittel, um die Optimierung der notwendigen Schritte besser zu strukturieren. Das Modell lässt zudem Sicherheitslücken und Schwachstellen des Systems erkennen und bietet Vorschläge zur Erreichung einer höheren Sicherheitsstufe.

7.6.1 Grenzen der Methode

Eines der Probleme, die diese Methode aufgezeigt hat, ist die schwere Greifbarkeit und Messbarkeit von Sicherheit. Sicherheit elektronisch gestützter Systeme kann nicht in absoluten Zahlen gemessen werden. Man kann nie sagen, dass ein System hundertprozentig sicher ist, genauso wenig, wie man hundertprozentig sichere Systeme herstellen kann. Zu viele Faktoren haben Einfluss auf die Sicherheit, man bedenke nur den Softwareentwicklungsprozess, bei dem nie ausgeschlossen werden kann, dass die hergestellte Software noch Bugs enthält (siehe auch Kapitel 3.3.3).

Das *Rice Theorem* besagt zudem, dass es nicht möglich ist, einen nicht trivialen Aspekt (wie die Korrektheit der Sicherheit) des funktionalen Verhaltens einer Turingmaschine (oder eines Algorithmus) algorithmisch zu überprüfen. Somit sind Sicherheitslücken wie auch Softwarefehler in Computersystemen niemals auszuschließen [McGr06, S. 108f].

Diese Methode zeigt somit auch die Grenzen einer Sicherheitsbewertung auf. Selbst, wenn mit dieser Methode ein guter Wert geschätzt werden konnte (ein E-Voting-System wurde auf einer vollständig grünen EVSSO-Matrix eingestuft), so kann trotz dieser guten Bewertung eine Sicherheits-

lücke nie ausgeschlossen werden. Grund dafür ist zum einen die inhärent unsichere zeitgenössische Technik und auf der anderen Seite der menschliche Faktor, der von Natur aus nur schwer berechenbar ist.

Das Ziel, auf das bei der Systementwicklung hingearbeitet wird und auf das mit dieser Methode verwiesen wird, ist, ein Computersystem so gut und so sicher wie nur möglich zu gestalten, allerdings ist Sicherheit selten vollständig zu erreichen (zudem bei komplexen Systemen unmöglich formal zu beweisen). So können Design-Fehler unentdeckt bleiben oder Software-Bugs schleichen sich ungewollt ein.

David Dill bemerkte zu diesem Thema einmal:

> „[..] finding cleverly hidden malicious code is much harder than finding a needle in a haystack.“ [Dill05]

Mat Bishop sagte ebenfalls:

> „[..] one can never verify that a system has no flaws, even if all source code is available.“ [BaBi07, S. 21]

Durch einen checklisten-artigen Aufbau erhöht man allerdings die Wahrscheinlichkeit, dass Systeme eine bestimmte Eigenschaft erfüllen.

7.6.2 Dimensionen der Sicherheit

Ein entscheidendes Merkmal der Bestimmung des Grades der Sicherheit eines Systems wie das eines E-Voting-Systems sind die verschiedenen Dimensionen, in der die Sicherheit betrachtet werden kann. Als Basis für die Bewertung der Sicherheit eines elektronischen Wahlsystems wurden die drei Hauptbereiche Hardware, Software und die Human Factors herangezogen. Nun erweist sich das Bestimmen des Sicherheitslevels einer der 16 beschriebenen Komponenten durch den checklistenartigen Aufbau recht einfach: Man betrachtet jeden Kernbereich und evaluiert die Sicherheitsstufe, um den Kernbereich einzuschätzen.

Geht man nun einen Schritt weiter und versucht nun auch die Sicherheit der Schnittstellen zwischen den Hauptbereichen zu evaluieren, wird das betrachtete System weit komplexer und es ergeben sich - rein mathematisch - 16 über 2, also 120 Kombinationsmöglichkeiten zwischen den einzelnen Kernbereichen. So wächst die Komplexität des betrachteten Systems enorm an. Versucht

man nun den Einfluss jeder Komponente auf das System und die Gesamtsicherheit zu bewerten, scheitert man letztendlich an der Vielschichtigkeit des Systems (siehe oben, Kapitel 7.6.1).

Es lässt sich somit sagen, je weiter unten (im Sinne von Komplexität) man ansetzt, desto einfacher ist es den Sicherheitsreifegrad zu bestimmen. Je komplexer sich das System nach oben entwickelt, desto schwieriger wird es.

Analog kann man die Entwicklung der Stufen der Komplexität von der kleinen Basis der mathematischen Problematik über die Hardware, Software, die Human Factors bis hin zum komplexen Gesamtsystem betrachten.

Die Grundlagen eines elektronischen Wahlsystems, die Kryptografie wie auch das verwendete Wahlprotokoll, also die mathematischen Grundladen sind noch relativ leicht in Bezug auf deren Sicherheit abzuschätzen und sind sogar noch formal beweisbar. Geht man nun eine Dimension weiter, eine Komplexitätsstufe höher im hier vorgestellten *Schalenmodell* (siehe Abbildung 28) und nimmt die Software zu der Mathematik dazu, ist die Abschätzung der Sicherheit nicht mehr trivial, da die Implementierung der mathematischen Regeln und Abläufe in einem komplexen Konstrukt fehlerbehaftet ist (vgl. *Rice Theorem* in Kapitel 7.6.1). Will man die Sicherheit zuzüglich der Hardware betrachten, nimmt die Komplexität des abzuschätzenden Teils wieder enorm zu, da nicht nur die Hardware für sich allein betrachtet werden muss, sondern auch die die Schnittstellen zwischen Hardware und Software, also Treiber, Firmware, Compiler, Betriebssystem, COTS-Produkte, etc.

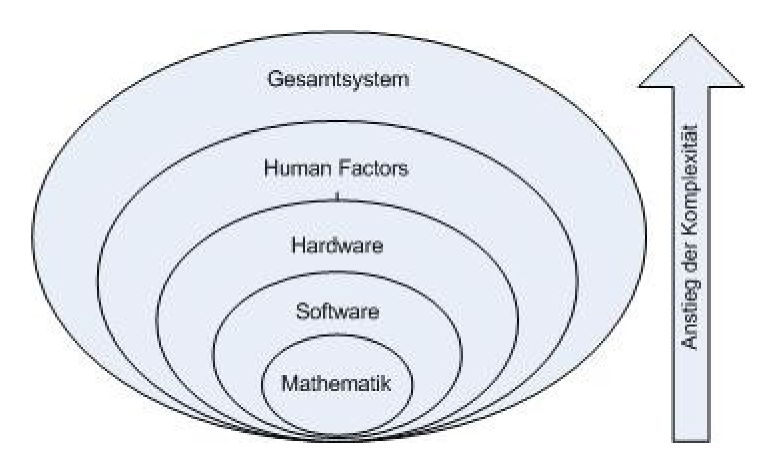


Abbildung 28: Schalenmodell analog zur EVSSO-Methode

Nimmt man nun auch noch die Human Factors in den Beobachtungsraum hinein, sind nicht nur die Schnittstellen zwischen Mensch und Maschine, sondern auch die Schnittstellen zwischen Mensch und Software, und die Verbindungen unter den Individuen zu betrachten. Die Komplexität steigt weiter extrem an.

Will man nun das Gesamtsystem betrachten, muss man jedes Einzelteil des Systems für sich, wie auch seinen Einfluss auf das gesamte System betrachten, wobei der Aufwand für eine vollständige Analyse derart exponentiell anwächst, dass das Problem der Analyse der Sicherheit des Gesamtsystems nicht mehr lösbar wird.

Das Schalenmodell analog zur EVSSO-Methode veranschaulicht somit den enormen, exponentiellen Anstieg der Komplexität bei der Analyse eines E-Voting-Systems in Hinblick auf dessen Sicherheit. Es zeigt zudem, dass je vielschichtiger ein System ist, desto schwieriger (bis hin zu unmöglich) wird es den Reifegrad der Sicherheit dieses Systems zu bewerten.

8 Conclusio und weitere Anmerkungen

Sicherheit zu bewerten ist generell ein schwieriges Unterfangen, da sich Sicherheit nur schwer quantifizieren lässt. Die vorgestellte Methode zur Bewertung und Optimierung der Sicherheit von E-Voting-Systemen (siehe Kapitel 7) bietet ein qualitatives Bewertungsverfahren, das nicht auf Klassifizierungen basiert, sondern sich auf die Visualisierung des Sicherheitsreifegrades stützt. Weiters lassen sich mit diesem Verfahren konkrete Schritte für die Erhöhung der Sicherheit bestimmen und unterschiedliche E-Voting-Systeme miteinander vergleichen. Die Methode unterscheidet sich von anderen, indem sie auf ganzheitlicher Sicherheit basiert, wobei die Hauptbereiche Hardware, Software und Human Factors eines E-Voting-Systems berücksichtigt werden, und eine visuelle Bewertung der Situation der Sicherheitsqualität ermöglicht, ohne konkrete Kategorisierungen zu verwenden. Das Verfahren ist als Ansatz für (staatliche) Zertifizierungen oder für die Verbesserung des Entwicklungsprozesses beim Hersteller gedacht.

Gleichzeitig zeigt die Methode aber auch die Grenzen der Sicherheitsbewertung komplexer Systeme auf. Neben den erörterten Sicherheitsproblemen (siehe Kapitel 5) und deren möglichen Gegenmaßnahmen (siehe Kapitel 6) ergibt sich auch die Frage, ob die derzeit verfügbare Soft- und Hardware überhaupt schon sicher genug ist, um für ein derartig kritisches Szenario wie elektronische Wahlen eingesetzt zu werden. Einige Kritiker behaupten, dass ausreichende Sicherheitskonzepte und Sicherheitsmechanismen mit dem heutigen Stand der Technik überhaupt nicht möglich seien und dass heutige elektronische Systeme inhärent fehlerhaft seien [Ston03, EvPa04].

So schätzt auch Sicherheitsexperte Klaus Brunnstein[90] eine merkbare Steigerung der Sicherheit in der IT-Branche erst in 20 Jahren ein, „bis die Unfälle so gravierend geworden sind, dass man die Sicherheitsdefizite nicht mehr akzeptiert". Die Computertechnik durchläuft die gleichen Zyklen wie jede andere technologische Veränderung: Zuerst gibt es Hoffnung, dass die neue Technologie Probleme lösen wird, dann Verzweiflung, weil die Technologie die hohen Erwartungen nicht erfüllt, und letztendlich greift ein regulatorisches Element (etwa staatliche Behörden) ein, um die neue Technologie in die Gesellschaft zu integrieren [Spar01].

Viele Sicherheitsexperten (darunter Aviel Rubin) schlagen als Alternative (zu DRE-Wahlsystemen) den gängigen Wahlvorgang mit Papierstimmzettel mit minimalem Einsatz von Technologie vor (etwa Ballot-Marking Machines, siehe Kapitel 6.10.1). Papierstimmzettel, egal ob die Stimmen elektronisch / mechanisch oder manuell erfasst, zusätzlich elektronisch gezählt, gescannt oder anders verarbeitet werden, bieten nicht nur den Wählern die Möglichkeit zu überprüfen, ob ihre Wahlentscheidungen auf adäquate Weise erfasst wurden, sondern können auch in einem öffentlich verfügbaren,

[90] Interview von Kurt Sagatz geführt mit Kurt Brunnstein in „Der Tagespiegel", Printausgabe vom 12.5.04.

transparenten Verfahren (erneut) ausgezählt werden - solange die Papierstimme als der Ausdruck des Wählerwillens gilt und nicht das elektronische Abbild.

Ein weiterer Aspekt bei elektronischen Wahlen ist ein Widerspruch, der in E-Voting steckt, denn die Stimmabgabe soll geheim bleiben, aber andererseits soll sie auch kontrollierbar bleiben, um Manipulationen auszuschließen. Datenschutz-Experte Hans Zeger meinte dazu:

> „Es gibt kein System, es ist auch vom Grundsatz denkunmöglich, dass beiden Anforderungen, nämlich Geheimhaltung und gleichzeitig auch Kontrolle, wer gewählt hat, entsprochen wird.“[91]

Eine wichtige Überlegung ist, *aus welchem Grund* E-Voting die gängigen Papierstimmzettel ersetzen sollte[92]. Ein Argument der Vertreter von E-Voting ist, dass traditionelle Wahlverfahren ebenfalls Sicherheitslücken enthalten (etwa Stimmenkauf mit Briefwahl, Kameras in Wahlzellen), die teilweise mit elektronischen Verfahren gesichert werden könnten.

Oft wird das *Arrow* Theorem[93] als Argument pro E-Voting oder als Hinweis erwähnt, dass bei Wahlen niemals alle Wahlgrundsätze zu 100 % eingehalten werden könnten, allerdings wird das Theorem oft falsch zitiert. Das Theorem besagt, dass es kein Wahlverfahren gibt, das einige grundlegende Bedingungen (Bedingung des unbeschränkten Bereichs, das schwache Pareto-Prinzip, Bedingung der Unabhängigkeit von irrelevanten Alternativen und der Nicht-Diktatur) erfüllt, allerdings bezieht es sich weder auf Sicherheit noch auf Transparenz oder andere Aspekte, die beim Vergleich von herkömmlichen Wahlen und E-Voting umstritten sind. Die meisten Argumente der Befürworter werden von Gegnern ziemlich leicht entkräftet (siehe auch Kapitel 1.3.1).

Die größten Probleme von E-Voting sind das Vertrauen und die Akzeptanz, die fehlende Transparenz des Vorganges (was macht die Maschine / der Computer wirklich? Wurde meine Stimme wirklich so, wie ich sie abgegeben habe, aufgenommen?), keine oder unzulängliche Papierbackups für erneute Auszählungen, fehlende Nachweisbarkeit über die Manipulationsfreiheit des Systems, schlechte Usability, fehlende Kontrolle für die Wahlkommission (vom Sourcecode bis zum Transfer der Stimme), das blinde Vertrauen in die Soft- und Hardware und nicht zuletzt die Sicherheit des gesamten Systems.

Ein unbestechbarer Vorteil der herkömmlichen Wahlen ist die Einfachheit des Ablaufes. Die Stimmabgabe mit Papierstimmzettel, Wahlkabine und Urne ist derart simpel gestaltet, dass sie

---

[91] Artikel in „Der Standard“ vom 04. Juni 2007.

[92] Der erfahrene Computer-Spezialist kennt die Regel „never change a running system!“.

[93] Kenneth J. Arrow beschrieb das Arrow-Theorem (auch „Arrow-Paradox“ oder „Allgemeines Unmöglichkeitstheorem“ genannt) erstmals 1951 in dem Buch „Social Choice and Individual Values“ und bekam für dieses Theorem 1972 den Nobelpreis für Wirtschaftswissenschaften.

auch ein Volksschüler verstehen kann. Bei E-Voting-Systemen ist die Kenntnis des genauen Ablaufes nur wenigen Experten vorbehalten, in technischen Details kann sich allerdings auch der beste Programmierer verstricken, zumal Fehler nicht hundertprozentig ausgeschlossen werden können (vgl. 7.6.1 Grenzen der Methode).

Somit bleibt die Frage, ob das bestehende funktionierende Wahlverfahren überhaupt ersetzt werden soll, noch offen. Andere Beispiele wie die Einführung des *Elektronischen Akts* (ELAK) im Bund zeigen, dass die Umstellung vom üblichen System auf ein elektronisches weit mehr Fallstricke beinhalten kann als ursprünglich angenommen.

Die Einführung von E-Voting in Österreich ist nach mehreren Pilotversuchen und ministeriellen Arbeitsgruppen und der Änderung des Wahlrechts hin zur Briefwahl - wenn es nach bestimmten Entscheidungsträgern gehen soll - nur noch eine Frage der Zeit. Nach einer OGM Umfrage[94] zum Thema E-Voting sprachen sich allerdings die absolute Mehrheit der befragten Österreicher (58 %) gegen elektronische Stimmabgaben bei Wahlen aus, nur 35 % befürworteten E-Voting. Der ehemalige VfGH-Präsident Korinek hat sich ebenfalls dezidiert gegen E-Voting ausgesprochen[95].

Offen bleibt noch, wann der Gesetzgeber die endgültige Änderung und Adaption des Wahlrechts beschließt, sodass der Empfehlung des Europarats für E-Voting-unterstützte Wahlen [CoE04] nachgekommen werden kann (siehe auch Kapitel 6.8.4). Somit betrifft die Frage der Sicherheit elektronisch gestützter Systeme und die Umsetzung von Wahlverfahren in Zukunft alle österreichischen Staatsbürger.

[94] OGM-Umfrage für die Zeitschrift Profil vom 17.11.2007.

[95] Interview in der ORF-"Pressestunde" vom 4.11.2007.

Appendizes

Appendix A: Die EVSSO-Checkliste

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
Hardware			
1	**Einhaltung der Wahlgrundsätze**		
1.A.1	Geheimes Wahlrecht: keine lineare / zeitliche Rückverfolgbarkeit, kein sequenzielles Ausdrucken der Stimmzettel etwa auf einer Endlos-Papierrolle.		
1.A.2	Geheimes Wahlrecht: Verwendung von Wahlkabinen mit Sichtschutz (auch nach oben) ohne Spiegel oder Kameras.		
1.B.1	Öffentlichkeit und Transparenz: Zugriff auf Geräte, Speichermedien und deren Dokumentation für Mitarbeiter oder Mitarbeiterinnen der Wahlkommission und Wahlbeobachter.		
1.B.2	Zugriff auf Geräte und Speichermedien beim Aufbau und beim Einsatz limitieren (Ausweiskontrollen, Schlüsselkarten, Überwachungspersonal oder ähnliches), Wahlkommission hat die Aufsicht.		
1.C.1	Lagerung, Sperrung und Versiegelung der Geräte und der Speichermedien, regelmäßige Überprüfung und Dokumentation der Sicherheitsvorkehrungen (Schlösser, Alarmanlagen, Bewegungsmelder, Überwachungspersonal, Hunden, etc.).		
1.C.2	Geheimes Wahlrecht: Schutz vor TEMPEST Attacken[96] durch emmissionsabsorbierende Kabinen oder weißes Rauschen und Minimierung des Geräuschpegels durch eine entsprechende Konstruktion der Wahlkabinen.		
2	**Safety**		
2.A.1	Korrektheit der Konstruktion. Konstruktion nach den aktuellen Standards der Technik. Überprüfung durch Abnahmetests.		
2.A.2	Homogene Architektur. Gleiche Hardware wird bei allen Geräten verwendet.		
2.A.3	Sicherheit der Konstruktion und Installation. Schutz vor Stromschlägen, Stolpern über Kabel, scharfen Kanten und anderen Verletzungen. Prüfung durch TÜV, CE-Kennzeichnung erforderlich.		
2.B.1	Belastbarkeit. Robuste Konstruktion durch Verwendung qualitativ hochwertiger Materialien, Kühlung der Komponenten, Schutz vor mechanischen, klimatischen und elektromagnetischen Umgebungseinflüssen.		

[96] TEMPEST Attacken basieren auf dem Abfangen und Analysieren der emittierten Strahlung der Geräte.

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
2.B.2	Haltbarkeit, Funktionssicherheit. Handbuch für den ordnungsgemäßen Gebrauch der Geräte vom Hersteller muss vorhanden sein und Richtlinien vorsehen, die eingehalten werden müssen.		
2.B.3	Schutz bei Transport und Aufbewahrung. Schutz vor Naturkatastrophen, Sicherung der Lagerräume, des Transports und der Aufstellung beim Einsatz der Geräte vor Fluten, Erdbeben, Stürme, Feuer, Kälte, etc. durch robuste, wasserfeste, hitzebeständige, erschütterungsresistente Schutzverpackungen bzw. gesicherte Aufbewahrungsorte mit Feuer- oder Rauchmeldern, (automatischen) Feuerlöscher, Wassersensoren, Klimaanlagen, Videoüberwachung, Bewegungsmelder und eventuell Erdbebenvorwarnsysteme. Regelmäßige Wartung der Schutzeinrichtungen.		
2.B.4	Energieversorgung. Schutz bei kurzfristigem Stromausfall, Spannungsspitzen oder -abfällen. Notfallsysteme (Generatoren, Akkus, Battery Backup Units, etc.) und Stromregulatoren installieren und warten.		
2.C.1	Erstellung eines Notfallplans*[*], Bildung eines Teams für die Durchführung eines Sicherheitsprogramms*, regelmäßiges Training des Personals für den Notfall.		
2.C.2	Rückwirkungsfreiheit der Schnittstellen. Keine unzulässige Beeinflussung der Messwerte im eichpflichtigen Messgerät möglich. Verwendung abgeschirmter Strom- und Netzwerkkabel.		
3	**Security**		
3.A.1	Schutz vor absichtlichen physikalischen Attacken wie Stromausfall, Wasserschäden, Beschädigung, Vandalismus, Diebstahl. Qualität der verwendeten Materialien und Werkstoffe bieten ausreichenden Schutz vor Attacken. Verschließbare Türen und Fenster am Aufbewahrungsort.		
3.A.2	Keine Internetverbindung(-smöglickeit). Entfernung von Netzwerkkarten und Versiegelung der Maschinen (Schlösser oder sichere Plomben).		
3.A.3	Entfernen nicht benutzter Geräte, etwa DVD-Laufwerke, Floppy-Laufwerk, WLan-Adapter, USB-Schnittstellen, etc.		
3.A.4	Zutrittskontrolle zu Maschinen: Der Zugang zu den Verwaltungsmaschinen (Applikationsserver, Datenbankserver oder Ähnliches) muss streng limitiert und überwacht werden (Ausweiskontrollen, Schlüsselkarten, Videoüberwachung, Bewegungsmelder, Alarmanlage, Warnzeichen, Flutlichtanlage, Überwachungspersonal, Wachhunde und Ähnliches). Regelmäßige Wartung der Schutzeinrichtungen.		

[*] Anmerkung: Eine detaillierte Beschreibung der Pläne (Sicherheitsplan, Notfallsplan, Zeitpläne, etc.) und Konzepte (Sicherheitskonzept etc.) würde den Rahmen dieser Arbeit sprengen, daher werden die Pläne hier nicht näher spezifiziert. In einschlägiger Sicherheitsliteratur, Softwareentwicklungshandbüchern, wie auch etwa im IT-Grundschutz Handbuch des BSI sind genaue Beschreibungen dieser Pläne zu finden.

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
3.B.1	Schutz der Speichermedien vor physikalischen Attacken, Entfernbarkeit der Module durch sichere Schlösser (keine Plomben) beschränken, Seriennummern, um Kopien der Speichermedien (Smartcards der Wähler und der Administration) zu erkennen.		
3.C.1	Schutz vor (internen) Denial-of-Service Attacken. Redundante Systeme (etwa RAID Festplattenverbund), Datenbank-Cluster, Load Balancer für die Applikation, Backups.		
3.C.2	BIOS Passwörter setzen. Booten von CD ausschließen.		
4	**Kryptografie**		
4.A.1	Verwendung sicherer, anonymer Verbindungen. Verwendung einer Technik zur Anonymisierung der Datenverbindung, z. B. Onion Routing[97], anonymes VPN oder anonymer Proxy.		
4.B.1	Hardware-Verschlüsselung der Festplatten.		
Software			
5	**Einhaltung der Wahlgrundsätze**		
5.A.1	Allgemeines Wahlrecht: korrekte Erfassung der Bürger in der Wählerevidenz. Nach Anmeldung zur digitalen Wahl wird der Wähler in die Wählerevidenz für E-Voting aufgenommen.		
5.A.2	Gleichheit: ein Stimmzettel pro Wähler, die Stimmen zählen gleich viel. Authentifizierung des Wählers, Kennzeichnung des (anonymen) Wählers, der einen Stimmzettel angefordert / abgegeben hat, auf der Smartcard (falls der Stimmzettel dort übergeben wurde) und im Wählerverzeichnis. Synchronisation einer lokalen Kopie der Wählerevidenz mit einer zentralen Datenbank, um mehrfache Stimmabgaben zu vermeiden.		
5.A.3	Geheimes Wahlrecht: anonyme Kanäle, verschlüsselte Kommunikation, anonyme authentische Stimmabgabe am Urnenserver durch Verwendung blinder, digitaler Signaturen. Keine lineare / zeitliche Rückverfolgbarkeit (keine sequenziellen Nummern), sondern Randomize-Funktion für Liste der abgegebenen Stimmen.		
5.B.1	Öffentlichkeit und Transparenz: Sourcecode der Software der Wahlmaschinen und der Wahlmanagement-Software durch Peer-Reviews (von technischen Experten) analysieren (lassen), Nachvollziehbarkeit der Stimmabgabe für Wähler durch Offenlegung des Sourcecodes, der Dokumentation und Zugang zu einem Bugtracking System. Die Ergebnisse der Analysen werden veröffentlicht.		
5.B.2	Eine öffentliche Liste der verwendeten Software (Betriebssysteme, COTS Produkte, Software, mit der das System entwickelt wurde, Firmware) inklusive der Version, Installationszeitpunkt und eine kurze Beschreibung.		
5.C.1	Öffentlichkeit und Transparenz: Sourcecode der Firmware, der Geräte-Treiber und der eingesetzten COTS-Produkte offenlegen.		

[97] Onion Routing [GoRe99] basiert auf David Chaum's Mix Networks [Chau81], wobei Daten über ständig wechselnde Routen über mehrere Nodes geschickt werden.

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
6	**Datenintegrität**		
6.A.1	Korrektheit der Implementierung von Stimmenspeicherung, Zählung und Anzeige: Abnahmetest nach Fertigstellung mit Abnahmeprotokoll. Reihenfolge der angezeigten Liste der Kandidaten muss mit der, die dem Bürger angezeigt wird, und der, die gespeichert wird, übereinstimmen. Anzahl der gezählten Stimmen pro Wahlgang muss mit der Anzahl der abgegebenen Stimmen übereinstimmen. Die abgegebene Stimme darf nicht kopiert, verändert oder fehlgeleitet werden und muss im Gesamtergebnis enthalten sein.		
6.A.2	Managementfunktionen und Audit-Funktionen der Wahlsoftware: • Zugriffskontrolle durch Authentifizierung mit „starken" Passwörtern, Chipkarten oder biometrische Daten • Allgemeine administrative Aufgaben: Verwaltung der Daten der Wahlkommissionsmitglieder, Importieren von Wahlgrunddaten (etwa im XML-Format), Bearbeiten von Wahlen (nur vor einer Wahl möglich) wie Ändern der Reihenfolge oder Wortlaut der Einträge der Kandidatenliste, Start und Stopp einer (Test-)Wahl, Überprüfung eines Wählers in der Wählerevidenz, Anzeige von Fehlern, Entschlüsselung der Stimmzettel (nur nach Beendigung der Wahl) und Start der (wiederholten) Auszählung. • Nur während einer laufenden Wahl ist eine Stimmabgabe möglich, Abfrage von inoffiziellen Zwischenergebnissen ist während der Wahl nicht möglich (bei Testwahlen schon).		
6.B.1	Schutz der Daten und Ausfallsicherheit: Verhindern eines Datenverlustes nach Absturz einer Maschine. Redundante Systeme, Cluster und Backups (Datenbanken, Zwischenspeicherung des Stimmzettels, Fehlen / Beschädigung des Sourcecodes, des Maschinencodes oder der Konfigurationsdateien) mit gleich hohen Standards wie die der originalen Systeme. Verwendung von Systemen (z. B. *Record Management Systeme* RMS) zur persistenten Speicherung temporärer Daten. Ausfall einer Maschine (Absturz) hat keinen Einfluss auf das Gesamtergebnis		
6.B.2	Verwendung synchronisierter, interner Uhren der Maschinen zum Abgleich der Wählerevidenz, Start und Ende der Wahl.		
7	**Kryptografie**		
7.A.1	Vertrauenswürdiger Pfad / Kanal: Verschlüsselung der Kommunikation durch Verwendung blinder, digitaler Signaturen.		
7.A.2	Schutz der Benutzerdaten und des Stimmzettels: Es darf nicht von außen ersichtlich sein, welcher Wähler bereits gewählt hat. Signierung der ausgegebenen Stimmzettel, Verschlüsselung vor Abgabe des Stimmzettels.		

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
7.A.3	Einsatz asymmetrischer Schlüssel (Chipkarten) für Identifikation, Authentisierung und Autorisierung: • Wahlberechtigungsprüfung: Identitätsprüfung, Abgleich und Kennzeichnung in der Wählerevidenz. • Stimmzettel-Authentizität: Nur auf signierten Stimmzetteln darf abgestimmt werden. (Blinde) digitale Signatur zur Zertifizierung der Authentizität nach Stimmauswahl, noch vor Stimmabgabe (vgl. Verfahren nach Fujioka et al.) • Stimmzettel-Verschlüsselung: Verschlüsselung des Stimmzettels mit symmetrischem Blindingfaktor zur Wahrung der Anonymität.		
7.B.1	Einsatz von „starken“ aktuellen Algorithmen. Etwa AES statt DES, SHA1-Hashes statt CRC (nicht verschlüsselt).		
7.B.2	Key Management. Sichere Speicherung, Aktivierung und Übertragung der Schlüssel.		
7.B.3	Methoden, um Kopien und Manipulationen der Speichereinheiten und Smartcards zu erkennen. Betrifft die Smartcards der Wähler und der Administration. Checks der Seriennummern und Signaturen. Verschlüsselung des Inhalts.		
7.C.1	Verschlüsselung von Konfigurationsfiles, der Festplatten der Geräte, der Daten auf den Speicherkarten und der Datenbanken.		
8	**Transparenz**		
8.A.1	Sourcecode und Dokumentation der Wahlsoftware zur Überprüfung durch Dritte verfügbar machen, Peer-Reviews durch unabhängige Experten. Ergebnisse der Reviews verfügbar machen.		
8.A.2	Wiederholte Testwahlen vor der rechtskräftigen Wahl auf einer kleinen Anzahl der Wahlgeräte (Stichprobe von 5 % der Maschinen, aber von mindestens 2 Geräten).		
8.B.1	Analyse der COTS-Produkte, des Betriebssystems und des BIOS mittels Peer-Reviews durch technische, unabhängige Experten. Die Ergebnisse werden veröffentlicht.		
8.B.2	Integration eines internen Fehleranalyse-Systems als Teil des E-Voting-Systems. Dieses System soll Warnungen, Fehler und Angriffe mit Zeitstempel und der betroffenen Komponente aufzeichnen.		
9	**Softwareentwicklung**		
9.A.1	Qualitätsmanagement: Reviews in jeder Phase des Entwicklungsprozesses, Dokumentation, Entwicklung und Einhaltung eines Zeitplans*.		
9.A.2	Risikomanagement in der Planungsphase: Benennung eines Sicherheitsbeauftragten und Erstellung eines IT-Sicherheitskonzeptes bzw. einer IT-Sicherheitsleitlinie*. Risikoanalysen und Assessment bereits in der Planungsphase durchführen. Ergebnisse in den Softwareentwicklungsprozess einfließen lassen.		

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
9.A.3	Nachvollziehbarkeit, ob ein anonymer Stimmzettel abgegeben wurde, durch nachträgliche Übertragung eines Dekodierschlüssels oder einer anderen eindeutigen Nummer in einem eigenen Schritt nach dem Versand des verschlüsselten ausgefüllten Stimmzettels. Die Stimmabgabe gilt bis zum letzten Schritt als nicht abgeschlossen und könnte neu begonnen werden.		
9.A.4	Überprüfung der Benutzereingaben auf (bösartig) fehlerhafte Eingabewerte. Nur validierter Input darf weiterverarbeitet werden.		
9.A.5	Interoperabilität mit bestehenden Systemen z. B. Schnittstellen zu bestehenden Systemen wie etwa das Zentralmelderegister nutzen und nicht neue Systeme als Ersatz für Bestehende entwickeln.		
9.B.1	Qualitätsmanagement: Automatische Testbarkeit (Unittests) bereits während der Entwicklung, manuelle Tests (Pen Tests, manuelle Inspektion) nach Abschluss eines Entwicklungszyklus bzw. Iteration durchführen.		
9.B.2	Allgemeine Implementierungsrichtlinien sind einzuhalten: • Fehlertransparenz (Exception Handling). • Schutz der administrativen Funktionen vor den Wählern: Login der Benutzer (ein Account darf nicht gleichzeitig von mehreren verwendet werden) und Verwendung von Benutzerrechten oder -rollen (Access Control Lists). Fehlerhafte Logins werden geloggt. Default-Passwort muss geändert werden und wird verschlüsselt gespeichert. • Sicherheitsprotokollierung von Fehlern, Abstürzen und Sicherheitsbrüchen. • Kommentare im Code: Code möglichst knapp halten, auf „hilfreiche“ Kommentare im Code achten (z. B. keine „FIXME“s). • Spezifikation und Dokumentation der Entwicklung. • Versionskontrolle (CVS oder SVN) verwenden.		
9.B.3	Security Tests und Auditing nach Implementierung: Durchführung von Black Box Tests mit Fuzzing[98].		
9.C.1	Teamaufteilung: duales Entwickeln.		
9.C.2	Security Tests und Auditing nach Implementierung: Review der Applikation auf Sicherheitsmerkmale, White Box Tests, Lasttests und Penetration Tests.		
9.C.3	Code Analysen mit Metriken nach Entwicklungszyklen / Iterationen durchführen zur Optimierung des SE-Prozesses.		
9.C.4	Interoperabilität für die Zukunft garantieren mit Verwendung offener, nicht proprietärer Standards (XML, Opensource, etc.).		
10	**Schutz der Software**		
10.A.1	Homogene Betriebssysteme. Alle Computer verwenden das gleiche OS, jeweils mit aktuellen Sicherheits-Updates.		

[98] Beim Fuzzing werden Zufallsdaten als Applikationsparameter übergeben.

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
10.A.2	Keine Default-Passwörter oder -PINs des Herstellers verwenden, lange „starke“ Passwörter aus Buchstaben, Ziffern und Sonderzeichen verwenden.		
10.B.1	Regelmäßige Überprüfungen der Version und der Integrität des Sourcecodes, der verwendeten externen (Standard-)Bibliotheken und der Konfigurationsdateien (mit digitalen Signaturen und Hash-Checks) vor, während und nach der Wahl.		
10.B.2	Sicherheit des Update-Mechanismus: Authentifizierung, Einschränkung des Zugriffs auf die Dateien und Freischaltung für ein Update.		
10.B.3	Nicht benötigte vorinstallierte Software deinstallieren (z. B. Mediaplayer oder FTP Clients).		
10.B.4	Skalierbarkeit: Durchführung von Lasttests mit Checks der benötigten Ressourcen und gegebenenfalls Änderung des Systemaufbaus.		
10.C.1	Überprüfung der Authentizität des Compilers mit Checksummen.		
10.C.2	Schutz gegen diverse (interne) Software Sicherheitsrisiken: gegen Buffer Overflows / Overrun, SQL / Sequal Injection, „Compiler Optimazation“ („Dead Store Removal“), Schutz vor Viren, Würmern, Trojanern, RootKits, Spyware, Keylogger, etc. mit Virenscannern, Firewalls, Intrusion Prevention Systems / Detection Systems, Honeypots[99] und div. anderen Protectiontools.		
10.C.3	Schutz vor Man-In-The-Middle Attacken durch Verschlüsselung der Übertragung oder Verwendung von Message Authentication Codes und verhältnismäßigen Netzwerkaufbau ohne Verbindung zum Internet oder anderen Netzen.		
Human Factors			
11	**Einhaltung der Wahlgrundsätze**		
11.A.1	Freies Wahlrecht: parteilose und neutrale Gestaltung des Stimmzettels und der Wahlmaschine. Es muss möglich sein ungültig zu wählen.		
11.A.2	Persönliches Wahlrecht: ohne Stellvertreter persönlich wählen.		
11.A.3	Allgemeines Wahlrecht: Aufklärung und Einschulung der Wähler in das E-Voting-System, Sicherstellung, dass die stimmberechtigte Person die Stimmabgabe versteht und durchführen kann.		
11.B.1	Öffentlichkeit und Transparenz: Einsichtnahme der Wahlkommission und Wahlbeobachter in Sourcecode und Zugang zu Wahlmaschinen		
12	**Sicherheitsmanagement**		

[99] Honeypots locken potenzielle Angreifer in Fallen, die wie begehrenswerte Angriffsziele aussehen oder wirken.

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
12.A.1	Einschulung des Personals und Erstellung von Sicherheitsplänen: Einschulung auf Sicherheitsmerkmale der Geräte und auf die Durchführung der regelmäßigen dokumentierten Tests, die vor, während und nach der Wahl an dem E-Voting-System durchgeführt werden. Stärkung des Sicherheitsbewußtseins, etwa von Social Engineering, Pigbacking-[100] und Insider Attacken. Definition von Rollen (Sicherheitsbeauftragter und Sicherheitsmanagement-Team) und eines Sicherheits- und Notfallplans* (was soll im Falle eines Ausfalles passieren, welche Rollen tragen die einzelnen Mitarbeiter, Notfallstrategien definieren, etc.).		
12.A.2	Sicherheitsmaßnahme: duale Kontrolle. Bei kritischen Maßnahmen ist die Autorisierung von zwei Mitarbeitern der Wahlkommission notwendig, z. B. Stornieren einer Stimme.		
12.A.3	Protokollierung der Handhabung von Software, Hardware und Stimmspeichermedien zur lückenlos nachvollziehbaren Kontrolle aller Prozesse.		
12.B.1	Hintergrund-Überprüfungen aller Mitarbeiter, die an der Entwicklung, an der Organisation und Administration beteiligt sind, vom Hersteller bis zur Wahlkommission und Wahlbeobachtern.		
12.B.2	Security Awareness Trainings aller (externen) Mitarbeiter, auch der Softwareentwickler, noch vor der Implementierung zur Risikovermeidung.		
13	**Benutzerinterface**		
13.A.1	Darstellung des Stimmzettels auf einer Bildschirmseite, ohne Scrollen.		
13.A.2	Anordnung der Parteien muss dem Papierstimmzettel entsprechen wie etwa Reihenfolge, Schriftgröße, Platzierung, etc.		
13.A.3	Adäquate Darstellung des Ablaufes der Stimmabgabe („Weiter“-, „Zurück“ und „Abbrechen“-Buttons, etc.), vor der endgültigen Abgabe kann der Stimmzettel nochmals kontrolliert und geändert werden. Übereilungsschutz muss gewährleistet werden. Klare Navigation.		
13.A.4	Keine Wahlbeeinflussung durch Werbung in Wahlkabinen oder am Display.		
13.A.5	Korrekte Darstellung des Stimmzettels. Kalibrierung bei Touchscreen-Geräten mit Überprüfungsmöglichkeiten, Reihenfolge der Kandidatenliste, gewählte Kandidaten stimmen mit den abgegebenen überein.		
13.A.6	Feedback für Benutzer während und nach Beendigung der Stimmabgabe.		
13.A.7	Online-Hilfe-Seiten bei jedem Schritt verfügbar. Benutzerhandbuch oder Anleitung in ausgedruckter Form. Kontextsensitive Online-Hilfe.		
13.A.8	Akzeptable Antwortzeiten der Applikation. Maximal 5 sec. pro Schritt.		
13.B.1	Mehrsprachigkeit der Applikation, der Dokumentation für den Wähler und der Hilfe.		
13.B.2	Vergrößerungen des Bildschirms (Lupe-Funktion) für Sehbehinderte.		

[100] Beim Piggybacking schleicht sich ein Angreifer mit einer autorisierten Person bei einem kontrollierten Zugang mit hinein.

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
13.B.3	Audio-Unterstützung für Blinde. Eventuell taktile Unterstützung.		
13.C.1	Usabilityprüfung mit einer repräsentativen Testgruppe und Dokumentation der Ergebnisse.		
14	**Transparenz**		
14.A.1	Bereitstellung von Informationen rund um die Wahl. Informationen über Kandidaten, die Funktionsweise des Wahlsystems, Zuordnung der Wähler zu Wahlsprengel, etc.		
14.A.2	Öffentliche Bekanntgabe der Bezirksergebnisse und Endergebnisse in Print- und Webmedien.		
14.A.3	Möglichkeit der Wahlbeobachtung vor, während und nach der Wahl. Anmerkung: Bei Stimmauszählungen in Österreich ist keine Wahlbeobachtung zum jetzigen rechtlichen Stand möglich.		
14.A.4	Überprüfung, ob die Anzahl der abgegebenen Stimmen mit der Anzahl der Wähler übereinstimmt, die einen Stimmzettel angefordert haben, und Definieren von Toleranzwerten, etwa 0,5 % Abweichung.		
14.A.5	Anonyme Papierbelege (*Voter-Verified Paper Trail*) für (erneute) Auszählungen bei Wahlanfechtungen und als Nachweis und zur Überprüfung für die Wähler. Die Papierbelege können nicht als Nachweis mitgenommen werden, sondern kommen in eine Urne und dienen als Backup der Stimmen.		
14.B.1	Auditphase der Wahlkommission nach der Wahl mit Lessons Learned für kommende Wahlen. Möglichkeit der Festhaltung von Fehlerberichten und Meinungen von Bürgern, die das System benutzt haben, Auswertung der Ergebnisse.		
14.B.2	Vergleich der Wahltagsbefragungen (*Exit Polls*) vom aktuellen und der vorangegangenen Jahre, Definition von Toleranzwerten, etwa maximal 10 % Abweichung.		
14.B.3	Bestimmung der Grenzwerte für manuelle Nachzählungen. Größe der Stichprobe (etwa 5 % der Papierstimmzettel) eines akzeptablen Toleranzwertes des Unterschiedes zum elektronischen Ergebnis bei manuellen Nachzählungen, etwa maximal 1 %.		
14.C.1	Ein öffentlich diskutierbares Wahlprotokoll und Verwendung von öffentlich verfügbare „starke“ kryptografische Algorithmen.		
15	**Gestaltung der Wahl**		
15.A.1	Die Registrierung zur elektronischen Wahl soll kein Hindernis etwa für ältere Menschen oder Menschen ohne Internetzugang darstellen.		
15.A.2	Parallelbetrieb: alternatives Wählen mit Papierstimmzettel möglich. Mehrfachabstimmungen vermeiden, indem Wählerevidenzen synchron gehalten werden.		
15.A.3	Zeitgleicher Beginn und Ende der elektronischen Stimmabgabe mit den konventionellen Wahlen.		
15.A.4	Verzögerungen des Ablaufes der Stimmabgabe verhindern: rechtzeitige Lieferung und Aufbau der Geräte und Einschulung der Mitarbeiter, etc.		

Nr.	*Kernbereich/ Anforderungen*	*OK*	*Anm.*
15.A.5	Möglichkeit einer Teststimmabgabe für einen Wähler, auch mit Anleitung eines Mitarbeiters der Wahlkommission.		
15.B.1	Akzeptanz und Verbreitung (Kostenfaktor): Kostentragungspflicht für die Geräte liegt bei öffentlichen Stellen.		
16	**Independent Testing Authority Validierung**		
16.A.1	Überprüfung, Zertifizierung oder Test durch unabhängige Prüf-Anstalten (Independent Testing Authority (ITA)) auf Korrektheit und Sicherheit. Offenlegung des Prüfberichts.		

Appendix B: E-Voting-Initiativen

Es gibt eine Reihe von Parteien, die sich für oder gegen E-Voting aussprechen. Hier wird ein Überblick über österreichische und internationale Initiativen, Vereine, Organisationen, Aktivisten und Experten gegeben.

Österreichische Initiativen

In Österreich gibt es eine Reihe von Initiativen, die sich mit IT-Sicherheit beschäftigen.

Der Verein Österreichische Computer Gesellschaft (OCG) hat einen Arbeitskreis *AK IT-Sicherheit*[101] gegründet, der sich mit den zentralen Aspekten der Sicherheit in der IT mit Schwerpunkt auf Safety von Systemen beschäftigt. Der Verein Initiative Informationssicherheit Austria (IISA)[102] hat eine Bewusstseinsbildung in Bezug auf Informationssicherheit in Unternehmen zum Ziel. Die Initiative Saferinternet.at bietet Informationen zum Thema Sicherheit im Internet und ist die österreichische Informations- und Koordinierungsstelle im Safer Internet Netzwerk der EU.

Zum Thema E-Voting gibt es in Österreich ebenfalls Seitens der OCG einen *Arbeitskreis eDemokratie/eVoting*[103], der 2002 gegründet wurde und unter der Leitung von Alexander Prosser der WU Wien steht. Der Arbeitskreis ist vor allem mit Publikationen und Veranstaltungen im Bereich E-Democracy tätig.

Alexander Prosser wirkt ebenfalls neben Robert Krimmer an der E-Voting-Initiative *e-Voting.at der Wirtschaftsuniversität Wien* mit. Die Initiative organisiert Pilotversuche und dient als Informationsplattform zum Thema E-Voting in Österreich. Der Pilotversuch einer elektronischen Testwahl via Internet für Auslandsösterreicher wurde mit Unterstützung vom Außenministerium (Thomas Buchsbaum), der Initiative e-Voting.at und der Wirtschaftsuniversität Wien durchgeführt (siehe Kapitel 4.5.1).

Robert Krimmer wiederum gründete den Verein *Competence Center for Electronic Voting and Participation (E-Voting.CC)*, der sich mit Beratung und Begleitung von E-Voting-Projekten und Wahlbeobachtungen, aber vor allem mit Organisation von E-Voting-Konferenzen beschäftigt. Als Verfechter von E-Voting-Systemen meinte er:

> „Die technischen und rechtlichen Aspekte sind gar nicht das Problem, sondern die Mittelsmänner, das heißt die Politiker, die für die Regulierung zuständig sind.“ [Siet07]

---

[101] http://www.ocg.at/ak/it-sicherheit/index.html

[102] http://www.iisa.at

[103] http://www.ocg.at/egov/edemocracy_evoting.html

Internationale Initiativen

Es gibt eine Reihe internationaler Initiativen für oder gegen E-Voting. Es folgt ein kurzer Überblick über diese Organisationen, Vereine und Aktivisten.

Europa

In Großbritannien ist die *Open Rights Group*[104], eine Organisation für Bürgerrechte im Internet, kritisch tätig. Im Juni 2007 wurde ein 60-seitiger Bericht [ORG07] zu Wahlbeobachtung der Pilot-Wahlversuche bei der Kommunalwahl im Mai 2007 in England und Schottland veröffentlicht. Die Organisation veranstaltete im Frühling 2007 den ersten *European Electronic Voting Activism Workshop* unter der Leitung von Jason Kitcat, bei dem internationale Kritiker von E-Voting eingeladen wurden.

Die Irische *Irish Citizens for Trustworthy Evoting ICTE*[105] setzte sich gegen den Einsatz der Nedap-Wahlmaschinen ein, befürwortet aber generell E-Voting.

Der *Chaos Computer Club* in Deutschland verhält sich gegenüber E-Voting ebenfalls kritisch und berichtete mit einer Wahlbeobachtergruppe von der Oberbürgermeisterwahl in Cottbus [Chao06]. Zudem wurde ein Gutachten zu Sicherheitslücken des Hamburger Wahlstiftes erstellt (siehe auch Kapitel 6.10.2).

Der Berliner Mathematiker Tobias Hahn startete im Herbst 2006 die Online-Bundestags-Petition gegen Wahlcomputer „Wahlrecht:Stimmabgabe mit Wahlgeräten", um die Abschaffung der gesetzlichen Grundlage für den Einsatz von Wahlcomputern (Streichung des § 35 im Bundeswahlgesetz) zu erzielen, die innerhalb sechs Wochen mehr als 45.000 Bürger unterzeichnet haben. Das Hauptargument der Petition war die fehlende Transparenz von E-Voting-Systemen, der Petition wurde allerdings nicht stattgegeben.

Eine Wahlprüfungsbeschwerde wurde beim Bundesverfassungsgericht vom Frankfurter Software-Spezialist Ulrich Wiesner mit der gleichen Motivation ebenfalls eingereicht, diese wurde ebenfalls abgewiesen.

Die französische Organisation *Ordinateurs De Vote*[106] des Informatikers Pierre Muller startete gegen den Einsatz von E-Voting-Systemen bei der Präsidentschaftswahl 2007 ebenfalls eine Unterschriftenliste, die knapp hunderttausend französische Bürger unterzeichnet haben, mit der zusätzliche Papierbelege, Audit-Verfahren und in letzter Folge den Verzicht auf Wahlmaschinen und die Beibehaltung von Papierstimmzetteln gefordert wird. Zusätzlich wurde bemängelt, dass bei den technischen Zulassungsbedingungen in Frankreich keine Quellcode-Inspektion der eingesetzten

---

[104] http://www.openrightsgroup.org

[105] http://www.evoting.cs.may.ie

[106] http://ordinateurs-de-vote.org

Software und keine Prüfmechanismen zur Verifikation der Integrität der E-Voting-Systeme verlangt werden.

Der holländische Aktivist Rop Gonggrijp gründete 2006 die Organisation *Wij vertrouwen stemcomputers niet*[107] ("Wir vertrauen Wahlmaschinen nicht"), die Kampagnen gegen Wahlsysteme ohne Voter Verified Paper Audit Trail startet. Gonggrijp führte im Oktober 2006 im Holländischen Fernsehen einen Hack auf eine E-Voting-Maschine des Herstellers Nedap vor und verfasste zudem eine Sicherheitsanalyse zu den Maschinen [GoHe06].

Die belgische Initiative *Pour une Ethique du Vote Automatisé*[108] setzt sich ebenfalls gegen den Einsatz von Wahlcomputern ein. Wahlcomputer werden in Belgien bereits seit 1994 verwendet.

USA

Ben Cohen initiierte die *The Computer Ate My Vote* Kampagne, die mit einer Unterschriftenliste, auf der mehrere hunderttausende US-Bürger unterschrieben haben, die Einstellung von Wahlen mit DRE-Maschinen und den Einsatz von Audit-Verfahren mit Papierbelegen fordert. Die U.S. Organisation *MoveOn* setzt sich mit ihrer Petition *Ban Paperless Voting*[109] wie auch Sheila Parks mit ihrer Forderung *Hand-Counted Paper Ballots Now* ebenfalls gegen E-Voting-Systeme ein. Das *Open Voting Consortium*[110] setzt sich für mehr Offenheit und die Verwendung von Papierstimmzettel ein. Der Verein *Common Cause*[111] ist 1970 zur „Verteidigung der Demokratie“ gegründet worden und unterstützt Bürger in politischen Fragen. E-Voting ist eines der Themen, mit dem sich diese beiden Vereinigungen auseinander setzen.

Die US-amerikanische *Electronic Frontier Foundation*[112] wurde 1990 gegründet und bildet eine Gruppe von Rechtsanwälten, Technikern und Freiwilligen, die sich für den Schutz der Bürgerrechte im Computerzeitalter und für faire und transparente Wahlen einsetzen. David Dill gründete die US-Amerikanische Organisation *Verified Voting*[113], die sich für vertrauenswürdige, zuverlässige und öffentlich verifizierbare Wahlen, ohne Einsatz von DRE-Wahlgeräten, einsetzt. *VoteTrustUSA*[114] ist ein Projekt der Verified Voting Foundation.

Mit der Organisation *Where's the Paper*[115] kämpft IT-Beraterin Teresa Hommel gegen die Anschaffung der holländischen Nedap-Wahlmaschinen in New York an. Sie schrieb zudem das Inter-

---

[107] http://www.wijvertrouwenstemcomputersniet.nl

[108] http://www.poureva.be

[109] http://pol.moveon.org/paperlessvoting

[110] http://www.openvotingconsortium.org

[111] http://www.commoncause.org

[112] http://www.eff.org

[113] http://verifiedvoting.org

[114] http://votetrustusa.org

[115] http://wheresthepaper.org

net-Applet *The Fraudulent Voting Machine*[116], mit dem gezeigt werden kann, wie einfach die Software manipuliert werden kann.

David Jefferson von der Cambridge Universität setzt sich wie auch Aviel Rubin von der Johns Hopkins Universität, Doug Jones von der Universität Illinois und Sicherheitsexperte Bruce Schneier gegen DRE-Systeme ein. Ed Felten und Alex Halderman von der Universität Princeton schreiben zusammen mit Dan Wallach von der Rice Universität das kritische Weblog *Freedom to Tinker*[117] über E-Voting-Technologie. John Schwartz von der NY-Times, Kim Zetter vom Wired Magazine[118] wie auch Aktivist und Blogger Brad Friedman[119] und Aviel Rubin[120] schreiben regelmäßig über Missstände bei E-Voting-Systemen in den USA. Bev Harris, die Aktivistin, die den Diebold Sourcecode im Internet auf einer neuseeländischen Seite entdeckte, gestaltet die Webseite *Black Box Voting*[121], die kritische Informationen zu politischen Prozessen rund um E-Voting enthält.

Die Vereinigung *A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections* (*ACCURATE*)[122] ist ein kollaboratives Projekt zwischen verschiedenen Institutionen, das sich auf kritische Untersuchungen von E-Voting-Systemen spezialisiert hat. ACCURATE untersucht Softwarearchitekturen, manipulationssichere Hardware, kryptografische Protokolle und Verifikationssysteme. Weiters beschäftigt sich die Organisation mit Usability und politischen Themen, um E-Voting sicherer zu gestalten. David Wagner von der UC Berkeley ist einer der Initiatoren des Programms.

Das *Caltech-MIT Voting Technology Project*[123] wurde von den Präsidenten der beiden Universitäten Caltech und Massachusetts Institute of Technology (MIT) gegründet, um in Zukunft die Probleme, die die erneute Auszählung bei den Präsidentschaftswahlen in den USA im Jahr 2000 verhindert haben, zu bewältigen. Wissenschaftler wie Ted Selker haben im Rahmen des Projekts eine Reihe kritischer Berichte zum Thema E-Voting veröffentlicht.

Kim Alexander gründete 1994 die Organisation *The California Voter Foundation*[124], einen unparteiischen Verein, der sich für einen Einsatz von Technologie zur Stärkung des demokratischen Prozes-

[116] http://www.uuvv.org/in.html

[117] http://www.freedom-to-tinker.com. Weitere Weblogs, die sich mit E-Voting auseinander setzen sind: http://blog.electiontechnology.com http://electionupdates.caltech.edu/blog.html http://electionlawblog.org http://moritzlaw.osu.edu/blogs/tokaji http://insideelections.shapethefuture.org http://www.edemocracy-forum.com http://allaboutvoting.com http://punchscan.org/blog

[118] http://www.wired.com

[119] http://www.bradblog.com

[120] http://avi-rubin.blogspot.com

[121] http://blackboxvoting.org

[122] http://accurate-voting.org

[123] http://www.vote.caltech.edu

[124] http://www.calvoter.org

ses einsetzt und sich kritisch gegenüber E-Voting äußert. *Voters Unite*[125] wie auch *Voter Action*[126] sind parteilose, non-profit U.S Organisationen, die sich für faire und akkurate Wahlen einsetzen. *Election Fraud News*[127] ist eine Organisation, die aus mehreren Wahlbetrugs-Experten und Wahlrechtsaktivisten besteht, die sich ebenfalls für freie und faire Wahlen in den USA einsetzt.

Auf der Webseite des *Election Incident Reporting System*s[128] können U.S. Bürger Vorfälle (Probleme, Irregularitäten, etc.) melden. Bisher wurden mehr als 30.000 Incidents gemeldet.
Der *Help America Vote Act (HAVA)*[129] stellt einen Meilenstein in der rechtlichen Entwicklung für den Einsatz von E-Voting dar. 2002 wurden durch HAVA 4 Millionen US-Dollar in die Aufrüstung auf E-Voting-Maschinen in den Vereinigten Staaten investiert. Die U.S. Gesetzgebung führte dadurch zu einem Einsatz von E-Voting bevor die Technologie ausgereift war. Die *US Election Assistance Commission*[130] wurde durch HAVA als Verrechnungs- und Informationsstelle eingesetzt.

Konstruktivere Ansätze kommen von David Wagner der Universität Berkeley und Ronald Rivest vom MIT (siehe auch Kapitel 6.7.2.2), die sich für sichere und vertrauenswürdige E-Voting-Systeme einsetzen.

Electionline[131] ist ein parteiloser Verein, der auf seiner Website aktuelle Informationen zu E-Voting bereitstellt. Die Organisation *The Election Center*[132] veranstaltet Konferenzen für Mitarbeiter von Wahlbehörden und Verkäufern von E-Voting-Systemen. Das Komitee *The National Committee for Voting Integrity*[133] vereint Experten aus verschiedenen Disziplinen, um transparente, sichere E-Voting-Systeme zu gestalten.

Daniel Tokaji, Assistenzprofessor am Ohio State Universität's Moritz College of Law, tritt ebenfalls für E-Voting-Systeme ein:

„From a voting rights perspective, electronic voting is better than the available alternatives“[134]

Brit Williams, Professor an der Kennesaw State Universität, war als Berater bei der Entwicklung der FEC-Standards (siehe Kapitel 6.9.2) tätig und gilt, wie auch Wahlkommissar Connie Schmidt von Johnson County, Kansas, USA, als Verfechter von DRE-Wahlmaschinen. Michael Shamos, ein Informatikprofessor an der Carnegie Mellon Universität, der E-Voting-Systeme aus Pennsylvania und

[125] http://www.votersunite.org

[126] http://www.voteraction.org

[127] http://www.electionfraudnews.com

[128] http://voteprotect.org

[129] http://www.fec.gov/hava/hava.htm

[130] http://www.eac.gov

[131] http://electionline.org

[132] http://www.electioncenter.org

[133] http://votingintegrity.org

[134] Interview mit Paul Festa: „E-voting: Nightmare or nirvana?“ für CNET News.com. 30. Juni 2004.

Texas inspiziert und zertifiziert hat, gilt ebenfalls als Verfechter von DRE-Maschinen und ist der Überzeugung, dass der Einsatz zusätzlicher Papierbelege E-Voting-Systemen nicht mehr Sicherheit bringen kann [Sham04].

Appendix C: Bibliographie

Kürzel	*Quelle*
Abe99	M. Abe: „Mix-networks on permutation networks“. In: Advances in Cryptology - ASIACRYPT '99, Lecture Notes in Computer Science, Vol. 1716. Springer, 1999. S. 258-273
ACM04	ACM Association for Computing Machinery: „ACM Policy Recommendations on Electronic Voting Systems“, September 2004
Acqu04	A. Acquisti: „Receipt-Free Homomorphic Elections and Write-in Ballots“. Technical Report International Association for Cryptologic Research 2004/105
AdDa00	J. Adler, W. Dai, R. Green, C. Neff. „Computational Details of the VoteHere Homomorphic Election System“. Whitepaper, ASIACRYPT, December 2000
AdRi06	B. Adida, R. Rivest: „Scratch & vote: self-contained paper-based cryptographic voting“. In: Workshop On Privacy In The Electronic Society. Proceedings of the 5th ACM workshop on Privacy in electronic society. SESSION: Private information management. 2006. S. 29-40
AiSc99	G. Aichhorn, R. Schmutzer: „E-Government: Elektronische Informationsdienste auf Bundesebene in Österreich. Endbericht (Studie im Auftrag des Bundeskanzleramts)“. In: Abschätzung der Österreichischen Akademie der Wissenschaften. Institut für Technikfolgen, 1999.
AlAr98	D. Alexander, W. Arbaugh, A. Keromytis, J. Smith: „Safety and security of programmable network infrastructures“. IEEE Communications Magazine, Special issue on Programmable Networks. 1998
Ande01	R. Anderson: „Why Information Security is Hard - An Economic Perspective“. In: Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual. 2001. S. 358-365
Appe06	A. Appel: „How to defeat Rivest's ThreeBallot Voting System“. Princeton University, October 5, 2006
Appe06a	A. Appel: „Ceci n’est pas une urne: On the Internet vote for the Assemblée des Français de l’étranger“. June 14, 2006, Rocquencourt, France
ArFo08	R. Araújo, S. Foulle, J. Traoré: „A practical and secure coercion-resistant scheme for remote elections (Extended Abstract)“. In: Dagstuhl Seminar Proceedings, Frontiers of Electronic Voting, Vol. 07311. IBFI, 2008
ArMo05	C. Armen, R. Morelli: „Evoting and Computer Science: Teaching About the Risks of Electronic Voting Technology“. In: Proceedings of the 10th annual SIGCSE conference on Innovation and technology in computer science education. Caparica, Portugal. SESSION: E-voting, ethics, and infrastructure for computing education. 2005. S. 227-231
BaBi07	E. Barr, M. Bishop, M. Gondree: „Fixing Federal E-Voting Standards“. In: Communications of the ACM, Volume 50, Issue 3 (March 2007). Emergency response information systems: emerging trends and technologies. Column: Viewpoint. 2007. S. 19-24
BaDu08	M. Backes, M. Dürmuth, D. Unruh: „Compromising Reflections or How to Read LCD Monitors Around the Corner“. In: IEEE Symposium on Security and Privacy, Proceedings of SSP'08,

Kürzel	*Quelle*
	July 2008
BaFa04	F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, A. Vaccarelli: „SEAS: A Secure E-Voting Applet System“. In: Software Security - Theories and Systems, Lecture Notes in Computer Science, Vol. 3233. Springer, 2004. S. 318-329
BaFo01	O. Baudron, S. Fouque, D. Pointcheval, G. Poupard, J. Stern: „Practical Multi-Candidate Election System“. In: Proceedings of the 20th ACM Symposium on Principles of Distributed Computing (PODC '01), N. Shavit Ed. ACM Press, 2001. S. 274-283
BaPi94	A. Baraani-Dastjerdi, J. Pieprzyk, R. Safavi-Naini: „A Practical Electronic Voting Protocol Using Threshold Schemes“. Center for Computer Security Research, Department of Computer Science, University of Wollongong, Australia, 1994
BaPr04	J. Bannet, D. Price, A. Rudys, J.Singer, D. Wallach: „Hack-a-vote: Security issues with electronic voting systems“. In: Security & Privacy Magazine, IEEE. Volume 2, Issue 1, Jan.-Feb. 2004. S. 32-37
Barb87	D. Barbara: „The Reliability of Voting Mechanisms“. In: IEEE Transactions On Computers, Vol. C-36, No. 10, October 1987. IEEE, 1987. S. 1197-1208
Bena87	J. Benaloh: „Verifiable Secret-Ballot Elections“. Yale University Department of Computer Science Technical Report number 561. 1987
Beno04	K. Benoit: „Experience of Electronic Voting Overseas“. In: First Report of the Commission on Electronic Voting, The Policy Institute, Trinity College Dublin. Commission on Electronic Voting, 2004. S. 311-326
BeTu94	J. Benaloh, D. Tuinstra: „Receipt-free secret-ballot elections“. In: Proceedings Of 26th Symp. on Theory of Computing (STOC’94), New York, 1994. S. 544-553
BeYu86	J. Benaloh, M. Yung: „Distributing the power of a government to enhance the privacy of voters“. In: Proceedings of the fifth annual ACM symposium on Principles of distributed computing, 1986. S. 52-62
BGBl02	Gesetz über die allgemeine und die repräsentative Wahlstatistik bei der Wahl zum Deutschen Bundestag und bei der Wahl der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland (Wahlstatistikgesetz - WStatG). Wahlstatistikgesetz vom 21. Mai 1999 (BGBl. I S. 1023), geändert durch Artikel 1 des Gesetzes vom 17. Januar 2002 (BGBl. I S. 412)
BGBl04	„Bundesgesetzblatt für die Republik Österreich“. Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG). Bundesgesetz, mit dem ein E-Government-Gesetz erlassen wird sowie das Allgemeine Verwaltungsverfahrensgesetz 1991, das Zustellgesetz, das Gebührengesetz 1957, das Meldegesetz 1991 und das Vereinsgesetz 2002 geändert werden (NR: GP XXII RV 252 AB 382 S. 46. BR: 6959 AB 6961 S. 705.) StF: BGBl. I Nr. 10/2004
BGBl07	„Bundesgesetzblatt für die Republik Österreich“. 28. Bundesgesetz: Wahlrechtsänderungsgesetz 2007 (NR: GP XXIII RV 88 AB 130 S. 24. BR: 7686 AB 7697 S. 746.) 28. Bundesge-

Kürzel	*Quelle*
	setz, mit dem die Nationalrats-Wahlordnung 1992, das Bundespräsidentenwahlgesetz 1971, die Europawahlordnung, das Wählerevidenzgesetz 1973, das Europa-Wählerevidenzgesetz, das Volksbegehrengesetz 1973, das Volksabstimmungsgesetz 1972 und das Volksbefragungsgesetz 1989 geändert werden (Wahlrechtsänderungsgesetz 2007)
BGBl30	„Bundesgesetzblatt für die Republik Österreich". Österreichisches Wahlrecht. Bundes-Verfassungsgesetz, BGBl.Nr. 1/1930 zuletzt geändert durch BGBl. I Nr. 27/2007
BGBl55	„Bundesgesetzblatt für die Republik Österreich". Staatsvertrag von Wien betreffend die Wiederherstellung eines unabhängigen und demokratischen Österreich, BGBl 1955/152
BGBl74	„Bundesgesetzblatt für die Republik Österreich". Bundesrecht - Strafgesetzbuch StGB, BGBl.Nr. 60/1974
BGBl92	„Bundesgesetzblatt für die Republik Österreich". Bundesgesetz über die Wahl des Nationalrates (Nationalrats-Wahlordnung 1992 - NRWO) BGBl.Nr. 471/1992
BGBl96	„Bundesgesetzblatt für die Republik Österreich". Europawahlordnung, BGBl.Nr. 117/1996
BGBl99	Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland. Bundeswahlgeräteverordnung vom 3. September 1975 (BGBl. I S. 2459), zuletzt geändert durch Artikel 1 der Verordnung vom 20. April 1999 (BGBl. I S. 749)
BGBl99a	„Bundesgesetzblatt für die Republik Österreich". Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG) (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.) StF: BGBl. I Nr. 190/1999
Bish05	M. Bishop: „Computer security - art and science". 7. print. Addison-Wesley, 2005
BiWa07	M. Bishop, D. Wagner: „Risks of e-voting". In: Communications of the ACM, Volume 50, Issue 11. COLUMN: Inside risks. ACM, 2007. S. 120
BKA07	Bundeskanzleramt: „Regierungsprogramm 2007 - 2010 - Regierungsprogramm für die XXIII. Gesetzgebungsperiode". 2007
BMI04	Bundesministerium für Inneres, Arbeitsgruppe „E-Voting": „Abschlussbericht". zur Vorlage an Dr. Ernst Strasser, Bundesminister für Inneres. Wien, 15. November 2004
Boeh91	B. Boehm: „Software risk management: principles and practices". In: Software, IEEE. Volume: 8, Issue: 1. 1991. S. 32-41
Boer04	J. Börcsök: „Elektronische Sicherheitssysteme - Hardwarekonzepte, Modelle und Berechnung". Hüthig, 2004
BoGo02	D. Boneh, S. Golle: „Almost Entirely Correct Mixing With Applications to Voting". In: Conference on Computer and Communications Security. Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002. S. 68-77
Bowe07	D. Bowen: „Withdrawal Of Approval Of Diebold Election Systems, Inc., GEMS 1.18.24/AccuVote-TSWAccuVote-OS DRE & Optical Scan Voting System And Conditional Re-Approval Of Use Of Diebold Election Systems, Inc., GEMS 1.18.24/AccuVote-TSWAccuVote-OS DRE & Optical Scan Voting System". Decertification/Recertification Decisions Issued August 3,

Kürzel	*Quelle*
	2007, by Secretary of State Debra Bowen. 2007
Bowe07a	D. Bowen: „Withdrawal Of Approval Of Hart Intercivic System 6.2.1 DRE & Optical Scan Voting System And Conditional Re-approval Of Use Of Hart Intercivic System 6.2.1 DRE & Optical Scan Voting System“. Decertification/Recertification Decisions Issued August 3, 2007, by Secretary of State Debra Bowen. 2007
Bowe07b	D. Bowen: „Withdrawal Of Approval Of Sequoia Voting Systems, Inc., Wineds V 3.1.012/AVC Edge/Insight/Optech 400-C DRE & Optical Scan Voting System And Conditional Re-approval Of Use Of Sequoia Voting Systems, Inc., Wineds V 3.1.012/AVC Edge/Insight/Optech 400-c Dre & Optical Scan Voting System “. Decertification/Recertification Decisions Issued August 3, 2007, by Secretary of State Debra Bowen. 2007
Boyd90	Boyd C: „A new multiple key cipher and an improved voting scheme”. In: Advances in cryptology - EUROCRYPT ’89. Springer, 1990. S. 617-25
Brad04	H. Brady: „Postponing the California Recall To Protect Voting Rights”. In: PS: Political Science & Politics, Vol. XXXVII, No. 1 (January). The American Political Science Association, 2004. S. 27-31
Bran05	G. Brands: „IT-Sicherheitsmanagement - Protokolle, Netzwerksicherheit, Prozessorganisation“. Springer, 2005
Brau03	N. Braun: „E-Voting in der Schweiz“. In: „e-Voting in der Schweiz, Deutschland und Österreich: Ein Überblick“. Working Papers on Information Processing and Information Management, Nr. 02/2003, Februar 2003. Internationales Rechtsinformatik Symposium - Session "e-Democracy/e-Voting". 2003. S. 11-16
BrBr06	N. Braun, D. Brändli: „Swiss E-Voting Pilot Projects - Evaluation, Situation Analysis and How to Proceed“. In: Proceedings of the 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC. Electronic Voting 2006. GI, 2006. S. 27-36
BrBu01	H. Brady, J. Buchler, M. Jarvis, J. McNulty: „Counting All The Votes : The Performance of Voting Technology in the United States“. Report, Department of Political Science, Survey Research Center, and Institute of Governmental Studies, University of California, Berkeley. September 2001
Bren04	Brennan Center for Justice: „Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems“. 28.06.04
BrJe01	S. Bruck, D. Jefferson, R. Rivest: „A Modular Voting Architecture (“Frogs”)“. Workshop on Trustworthy Elections WOTE '01, August 26 - 29, 2001, Marconi Conference Center. 2001
BrLi06	J. Bryans, B. Littlewood, S. Ryan, L. Strigini: „E-voting: Dependability Requirements and Design for Dependability“. In: Proceedings of the First International Conference on Availability, Reliability and Security (ARES’06). IEEE, 2006. S. 988-995
BSI05	BSI Bundesamt für Sicherheit in der Informationstechnik: „BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)“. Version 1.0, 2005

Kürzel	*Quelle*
BSI05a	BSI Bundesamt für Sicherheit in der Informationstechnik: „BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise“. Version 1.0. 2005
BSI05b	BSI Bundesamt für Sicherheit in der Informationstechnik: „BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz“. Version 2.0. 2005
BSI07	BSI Bundesamt für Sicherheit in der Informationstechnik: „Common Criteria Schutzprofil - Schutzprofil 'Digitales Wahlstift-System'“, V 1.0.1 BSI-PP-0031
BSI07a	BSI Bundesamt für Sicherheit in der Informationstechnik: „Zertifizierungsreport - BSI-PP-0031-2007 zu Schutzprofil Digitales Wahlstift-System, Version 1.0.1 entwickelt im Auftrag der Freien und Hansestadt Hamburg“. Zertifizierungsreport V1.0, ZS-01-01-F-301 V2.02. Vertrauenswürdigkeitspaket: EAL 3 mit Zusatz von ADV_SPM.1 und AVA_MSU.3, gültig bis 30.06.2008. BSI, 2007
BSI08	BSI Bundesamt für Sicherheit in der Informationstechnik: „BSI-Standard 100-4: Notfallmanagement“. Entwurf, Version 0.7. 2008
Buch04	T. Buchsbaum: „Abschlussbericht der Unterarbeitsgruppe 3 (E-Voting im internationalen Vergleich)“. Arbeitsgruppe E-Voting im BMI, Unterarbeitsgruppe Internationales. 2004
Bund05	16. Deutscher Bundestag: „Beschluss des 16. Deutschen Bundestags vom 14. Dezember 2006“. WP 145/05, BT-Drs 16/3600, 7 (Anlage 1) „Wahlcomputer“. Einspruch betreffend der Gültigkeit der Wahl zum 16. Deutschen Bundestag am 18. September 2005
CaBo05	L. Camp, W. Bowman, A. Friedman: „Voting, Vote Capture & Vote Counting Symposium“. In: ACM International Conference Proceeding Series; Vol. 89. Proceedings of the 2005 national conference on Digital government research, Atlanta, Georgia. SESSION: E-voting. 2005. S. 198-199
CaGr05	T. Carroll, D. Grosu: „A Secure and Efficient Voter-Controlled Anonymous Election Scheme“. In: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC’05). IEEE, 2005. S. 721-726 Vol. 1
Cast07	D. Castro: „Stop the Presses: How Paper Trails Fail to Secure e-Voting“. Report. The Information Technology & Innovation Foundation. 18.9.2007
CCC06	CCC Chaos Computer Club: „Bericht der CCC-Wahlbeobachtergruppe von der Oberbürgermeisterwahl in Cottbus“. 24.10.2006
CESG02	CESG Communications-Electronics Security Group: „E-Voting Security Study“, X/8833/4600/6/21, (Copyright The Crown) Issue 1.2 31 United Kingdom. 2002
Chau04	D. Chaum: „Secret-Ballot Receipts: True Voter-Verifiable Elections“. In: Security & Privacy Magazine, IEEE, Volume: 2, Issue: 1. 2004. S. 38-47
Chau81	D. Chaum: „Untraceable electronic mail, return addresses, and digital pseudonyms“. In: Communications of the ACM, Volume 24, Issue 2. 1981. S. 84-90
Chau82	D. Chaum: „Blind Signatures for Untraceable Payments“. In: Advances in Cryptology Proceedings of Crypto 1982, Plenum. Springer, 1982. S. 199-203
Chau88	D. Chaum: „Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Brea-

Kürzel	*Quelle*
	king RSA“. In: Advances in Cryptology - EUROCRYPT '88, Lecture Notes in Computer Science Vol. 330. Springer, 1988. S. 177-182
ChGo95	B. Chor, O. Goldreich, E. Kushilevitz, M. Sudan: „Private Information Retrieval”. In: Proceedings of the 36th IEEE Symposium on Foundations of Computer Science (FOCS), 1995. S. 41-50
ChHo05	C. Chen, C. Lan, G. Horng: „A Practical Voting System for Small-scale Election“. In: Information Technology: Research and Education, 2005. ITRE 2005. 3rd International Conference on, 2005. S. 322-326
ChRy05	D. Chaum, S. Ryan, S. Schneider: „A practical voter-verifiable election scheme“. In: ESORICS, Lecture Notes in Computer Science, Vol. 3679. Springer, 2005. S. 118-139
ClCh08	M. Clarkson, S. Chong, A. Myers: „Civitas: A Secure Remote Voting System“. In: Dagstuhl Seminar Proceedings, Frontiers of Electronic Voting, Vol. 07311. IBFI, 2008
CoE04	CoE Counil of Europe - Europarat: „Legal, Operational And Technical Standards For E-voting“. Die Empfehlung des Europarates zu E-Voting. Recommendation Rec(2004)11 vom 30 September 2004. Council of Europe Publishing, 2004
CoFi85	J. Cohen, M. Fischer: „A Robust and Verifiable Cryptographically Secure Election Scheme“. In: Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science, 1985. S. 372-382
CrCy97	L. Cranor, R. Cytron: „Sensus: A security-conscious electronic polling system for the internet“. In: Proceedings of the Hawaii International Conference on System Sciences. Wailea, Hawaii. IEEE Computer Society Press, 1997. S. 561-570 vol.3
CrFr95	R. Cramer, M. Franklin, B. Schoenmakers, M. Yung: „Multi-Authority Secret-Ballot Elections with Linear Work“. Technical Report: CS-R9571, CWI, 1995
CrGe97	R. Cramer, R. Gennaro, B. Schoenmakers: „A secure and Optimally Efficient Multi-Authority Election Scheme“. In: Advances in Cryptology - EUROCRYPT'97, Lecture Notes in Computer Science, Vol. 1233. Springer, 1997. S. 103-118
DaGr03	I. Damgård, J. Groth, G. Salomonsen: „The Theory and Implementation of an Electronic Voting System.“ In: Secure Electronic Voting. Kluwer Academic Publ., 2003. S. 77-99
DaHu92	W. Daenzer, F. Huber. (Hrsg.): „Systems engineering - Methodik und Praxis - 7. Aufl.“. Industrielle Organisation, 1992
DaJu01	I. Damgård, M. Jurik: „A generalisation, a simplification and some applications of paillier’s probabilistic public-key system“. In: Public Key Cryptography. PKC 01, 2001. S. 119-136
DaJu03	I. Damgård, M. Jurik, J. Nielsen: „A Generalization of Paillier’s Public-Key System with Applications to Electronic Voting“. Report of the Aarhus University, Dept. of Computer Science, BRICS. 2003
DBtg02	DBtg Deutscher Bundestag: „Geschichte des Wahlrechts - Der Kampf um gleiche Wahlen in Deutschland “. In: Blickpunkt 06/2002. Deutscher Bundestag, 2002.
DePe08	O. de Marnee, O. Pereira, J. Quisquater: „Simulation-based analysis of E2E voting systems“.

Kürzel	*Quelle*
	In: Dagstuhl Seminar Proceedings, Frontiers of Electronic Voting, Vol. 07311. IBFI, 2008
DePr07	D. De Cock, B. Preneel: „Electronic Voting in Belgium: Past and Future“. In: A. Alkassar and M. Volkamer (Eds.): VOTE-ID 2007, LNCS 4896. Springer-Verlag, 2007. S. 76-87
DiHe76	W. Diffie, M. Hellman: „New directions in cryptography“. In: IEEE Transactions on Information Theory, Volume: 22, Issue: 6. IEEE 1976, S. 644-654
Dill05	D. Dill: „Electronic voting: An overview of the problem.“ Talk presented to the Carter-Baker Commission on Federal Election Reform, Washington, D.C. (Apr. 18, 2005)
Dini02	G. Dini: „A secure and available electronic voting service for a large-scale distributed system“. In: Future Generation Computer Systems, Volume 19, 2003. S. 69-85
Dini02a	G. Dini: „Increasing Security and Availability of an Internet Voting System“. In: Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02), 2002, S. 347
DiPe04	A. Di Franco, A. Petro, E. Shear, V. Vladimirov: „Small vote manipulations can swing elections“. In: Communications of the ACM, Volume 47, Issue 10. Voting systems - SPECIAL ISSUE: The problems and potentials of voting systems. 2004. S. 43-45
DiRu04	D. Dill, A. Rubin: „E-Voting Security“. In: IEEE Security & Privacy Magazine, Volume 2, Issue 1. 1540-7993, IEEE Computer Society. 2004. S. 22
DiSc03	D. Dill, B. Schneier, B. Simons: „Voting and Technology: Who Gets to Count Your Vote?“. In: Communications of the ACM August 2003/Vol. 46, No. 8. ACM, 2003. S. 29-31
DiSi08	D. Dill, B. Simons: „The Democratic Party's Dangerous Experiment“. VoteTrustUSA 2.2.2008
DiWa07	D. Dill, D. Wallach: „Stones Unturned: Gaps In The Investigation Of Sarasota’s Disputed Congressional Election“. 13.04.2007
Dujm00	W. Dujmovits: „Auslandsösterreicherwahlrecht und Briefwahl“. Verlag Österreich. 2000
EAC05	EAC Election Assistance Commission: „Voluntary Voting System Guidelines“. 2005
EkDa95	L. Ekenberg, M. Danielson: „Handling Imprecise Information in Risk Management“. In: Proceedings of 11th IFIP SEC Conference. Chapman & Hall. 1995. S. 357-368
ElGa85	T. ElGamal: „A public-key cryptosystem and a signature scheme based on discrete logarithms“. In: Advances in Cryptology, Lecture Notes in Computer Science, Vol. 196. Springer, 1985. S. 10-18
Engu06	C.Enguehard: „Note technique sur les ordinateurs de vote“. Technischer Report. 8.12.2006.
ESI06	ESI Election Science Institute: „DRE Analysis for May 2006 Primary - Cuyahoga County, Ohio“. August 2006
Ever07	S. Everett: „The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection“. PhD Theses, Rice University. 2007
EvPa04	D. Evans, N. Paul: „Election security: Perception and reality“. In: Security & Privacy Magazine, IEEE,Volume: 2, Issue: 1. 2004. S. 24-31
FAA03	FAA Federal Aviation Administration: „Federal Register - Proposed Rules“. Department Of Transportation, Federal Aviation Administration. Federal Register. Vol. 70, No. 109. 14 CFR Part 27. 2005

Kürzel	*Quelle*
FEC01	FEC Federal Election Commission: „Voting Systems Standards“. Agenda Document Number 01-62 on the agenda for consideration at the December 13, 2001, meeting of the Federal Election Commission. 2001
FEC02	FEC Federal Election Commission: „Voting Systems Standards“. April, 2002
FeHa06	A. Feldman, J. Halderman, E. Felten: „Security Analysis of the Diebold AccuVote-TS Voting Machine“. Princeton University. 13.09.2006
FiCa06	K Fisher, R Carback, A Sherman: „Punchscan: Introduction and System Definition of a High-Integrity Election System“. In: Preproceedings of the IAVoSS Workshop On Trustworthy Electi-ons (WOTE'06). 2006. S. 19-29
Fire03	D. Firesmith: „Common Concepts Underlying Safety, Security, and Survivability Engineering“. CMU/SEI-2003-TN-033, Software Engineering Institute. 2003. S. 14
FiZu05	G. Fischer, W. Zuser: „The Vote Scrambling Algorithm“. In: Effizienz von e-Lösungen in Staat und Gesellschaft. Aktuelle Fragen der Rechtsinformatik. Boorberg Verlag, 2005
FoBe00	D. Fowler, S. Bennett: „IEC 61508 - A Suitable Basis for the Certification of Safety-Critical Transport-Infrastructure Systems??“. In: Computer Safety, Reliability and Security: Procee-dings of the 19th International Conference, SAFECOMP 2000, Rotterdam, The Netherlands, October 2000. Lecture Notes in Computer Science, Vol. 1943. Springer, 2000. S. 250-263
FrLu04	K. Frühauf, J. Ludewig, H. Sandmayr: „Software-Prüfung - Eine Anleitung zum Test und zur Inspektion“. 5. Aufl. Vdf-Lehrbuch. 2004
FuOk93	A. Fujioka, T. Okamoto, K. Ohta. „A practical secret voting scheme for large scale elections“. In: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology - AUSCRYPT '92. Lecture Notes in Computer Science, Vol. 718. Springer, 1993. S. 244-251
GaRo05	C. García-Zamora, F. Rodríguez-Henríquez, D. Ortiz-Arroyo „SELES: An e-Voting System for Medium Scale Online Elections“. In: Proceedings of the Sixth Mexican International Confe-rence on Computer Science. 2005. S. 50-57
GI07	GI Gesellschaft für Informatik: „Mitteilungen der Gesellschaft für Informatik 185. Folge“. In: Informatik-Spektrum, Volume 30, Number 3 / Juni 2007. Springer, 2007. S. 126
Gilm98	J. Gilmore ed.: „Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip De-sign“. O'Reilly, July 1998
Goeth17	Johann Wolfgang von Goethe: „Die guten Weiber“; A 9/428, 1817
GoHe06	R. Gonggrijp, W. Hengeveld, A. Bogk, D. Engling, H. Mehnert, F. Rieger, S. Scheffers, B. Wels: „Nedap/Groenendaal ES3B voting computer - a security analysis“. The “We do not trust voting computers” foundation. 6.10.2006
GoKl06	M. Gogolewski, M. Klonowski, S. Kubiak, M. Kutyłowski, A. Lauks, F. Zagórski: „Kleptogra-phic Attacks on E-Voting Schemes“. In: ETRICS 2006, Lecture Notes in Computer Science, Vol. 3995. Springer, 2006. S. 494-508
GoRe99	D. Goldschlag, M. Reed, S. Syverson: „Onion routing“. In: Communications of the ACM. Volu-

Kürzel	*Quelle*
	me 42, Issue 2. 1999. S. 39-41
GoZh02	P. Golle, S. Zhong, D. Boneh, M. Jakobsson, A. Juels: „Optimistic Mixing for Exit-Polls“, In: ASIACRYPT 2002, Lecture Notes in Computer Science, Vol. 2501. Springer 2002. S. 451-465
Grit03	D. Gritzalis: „Secure Electronic Voting: The current landscape“. In: Secure Electronic Voting. Kluwer Academic Publ., 2003. S. 101-122
Groe02	Å. Grönlund: „Private Sanctity - e-Practices Overriding Democratic Rigor in e-Voting“. In: R. Traunmüller and K. Lenk (Eds.): EGOV 2002, Lecture Notes in Computer Science, Vol. 2456. Springer, 2002. S. 52-60
Groe06	J. Groenendaal: „Wahlnachrichten der HSG Wahlysteme GmbH - Eine neue 'Aktionsgruppe' in den Niederlanden“. Statement dazu von Jan Groenendaal, Übersetzung aus dem Niederländischen. August 2006
Grov04	J. Grove: „ACM statement on voting systems“. In: Communications of the ACM, Volume 47, Issue 10, Voting systems. ACM, 2004. S. 69-70
Gyul06	L. Gyulai: „Plug pulled on electronic voting - High-tech balloting cost 25 per cent more“. The Gazette, 25.10.2006
Harr04	B. Harris „Black Box Voting: Ballot-Tampering in the 21st Century“. Talion Publishing. 2004
Hass01	V. Hassler: „Security fundamentals for e-commerce“. Artech House, 2001
Hein03	P. Heindl: „E-Voting und e-Democracy aus verfassungsrechtlicher Sicht“. In: Institut für Informationsverarbeitung und Informationswissenschaft, Wirtschaftsuniversität Wien (Hrsg.): e-Voting in der Schweiz, Deutschland und Österreich: Ein Überblick, Nr. 02/2003, Wien. 2003. S. 23-27
Hers97	M. Herschberg: „Secure Electronic Voting Over the World Wide Web“. Master’s Thesis, Massachusetts Institute of Technology, June 1997
HiSa00	M. Hirt, K. Sako: „Efficient Receipt-Free Voting Based on Homomorphic Encryption“. In: B. Preneel (Ed.): EUROCRYPT 2000, Lecture Notes in Computer Science, Vol. 1807. Springer, 2000. S. 539-556
HoBe00	H. Hochheiser, B. Bederson, J. Johnson, C. Karat, J. Lazar „The Need for Usability of Electronic Voting Systems: Questions for Voters and Policy Makers“. White Paper submitted to Computer Science and Telecommunications Board, US National Academy of Sciences, 2004
Hoff00	L. Hoffmann: „Internet voting: will it spur or corrupt democracy?“. In: Computers, Freedom and Privacy, Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions. ACM, 2000. S. 219-223
HoLa06	L. Hoffman, K. Lawson-Jenkins, J. Blum: „Trust Beyond Security: An Expanded Trust Model“. In: Communications of the ACM July 2006/Vol. 49, No. 7. ACM, 2006. S. 95-101
HoLe02	M. Howard, D. LeBlanc: „Writing secure code - practical strategies and proven techniques for building secure applications in a networked world“. Microsoft Press, 2002
Holt07	R. Holt: „H.R. 811: Voter Confidence and Increased Accessibility Act of 2007“. 2007-2008

Kürzel	*Quelle*
	(110th Congress). Introduced: 5.2.2007
Holz05	M. Holzbach: „Sichere IT in der Verwaltung“. In: A. Zechner (Hrsg.): E-Austria-Guide - E-Government, E-Learning, E-Health, E-Business. Linde, 2005. S. 186f
HoMi95	P. Horster, M. Michels, H. Petersen: „Blind multisignature schemes and their relevance for electronic voting“. In: Proceedings of COMPSAC'95, 1995. S. 149-155
HoSt06	I. Hogganvik, K. Stølen: „A Graphical Approach to Risk Identification, Motivated by Empirical Investigations“. In: O. Nierstrasz et al. (Eds.): MoDELS 2006, Lecture Notes in Computer Science, Vol. 4199. Springer, 2006. S. 574-588
HSG98	Hochschülerinnen- und Hochschülerschaftsgesetz HSG 1998 - (Bundesgesetz über die Vertretung der Studierenden). BGBl. I Nr. 22/1999, idF BGBl. I Nr. 95/1999, I/18/2001, I/1/2005, I/19/2005 (DFB), I/160/2006 (KM), I/12/2007, I/47/2007
Hump89	W. Humphrey: „Managing the Software Process“. Addison-Wesley, 1989
Hurs06	H. Hursti: „Diebold TSx Evaluation - SECURITY ALERT: May 11, 2006 - Critical Security Issues with Diebold Tsx“. Unredacted - Released July 2, 2006 by Black Box Voting. A Black Box Voting Project. 2006
IbKa03	S. Ibrahim, M. Kamat, M. Salleh, S. Aziz: „Secure E-voting with blind signature“. In: Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on on Telecommunication Technology, 14-15.10.2003. S. 193-7
IEEE01	IEEE Institute of Electrical and Electronics Engineers: „IEEE Voting Equipment Standard - Project Presentation“. 2001
IEEE90	IEEE Institute of Electrical and Electronics Engineers: „IEEE Computer Dictionary - Compilation of IEEE Standard Computer Glossaries, 610-1990“. 1990
IEEE98	IEEE Institute of Electrical and Electronics Engineers: „IEEE Guide for Information Technology-System Definition-Concept of Operations (ConOps) Document“. IEEE Std 1362-1998. 1998
INCO00	INCOSE International Council on Systems Engineering: „Systems Engineering Handbook“, Version 2.0, 2000
IPI01	Internet Policy Institute: „Report of the National Workshop on Internet Voting: Issues and Research Agenda“. March 2001
Iver92	K. Iversen: „A Cryptographic Scheme for Computerized General Elections“. In: Science, Advances in Cryptology — CRYPTO ’91, Lecture Notes in Computer, Vol. 576. Springer, 1992. S. 405-419
JaCh01	J. Jan, Y. Chen, Y. Lin: „The Design of Protocol for e-Voting on the Internet“. In: Security Technology, 2001 IEEE 35th International Carnahan Conference on. S. 180-189
Jako98	M. Jakobsson: „A Practical Mix“. In: Advances in Cryptology - EUROCRYPT '98, Lecture Notes in Computer Science, Vol. 1403. Springer, 1998. S. 448-461
JeRu04	D. Jefferson, A. Rubin, B. Simons, D. Wagner: „A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)“. 2004

Kürzel	*Quelle*
JeRu04a	D. Jefferson, A. Rubin, B. Simons, D. Wagner: „Analyzing internet voting security: An extensive assessment of a proposed internet-based voting system“. In: Communications of the ACM, Volume 47, Issue 10 (October 2004). S. 59-64
Jone01	D. Jones: „Problems with Voting Systems and the Applicable Standards“. Testimony before the House Science Committee, May 22, 2001
Jone03	D. Jones: „The Case of the Diebold FTP Site“. Part of the Voting and Elections web pages by The University Of Iowa, Department of Computer Science, 2003
Jone03	D. Jones: „The evaluation of voting technology“. In: Secure Electronic Voting. Kluwer Academic Publ., 2003. S. 3-16
Jone05	M. Jones: „The Pedagogic Opportunities of Touch-Screen Voting“. In: ACM SIGCSE Bulletin, Volume 37, Issue 3. SESSION: E-voting, ethics, and infrastructure for computing education. ACM, 2005. S. 223-226
JoRi08	R. Joaquim, C. Ribeiro: „CodeVoting: protecting against malicious vote manipulation at the voter's PC“. In: Dagstuhl Seminar Proceedings, Frontiers of Electronic Voting, Vol. 07311. IBFI, 2008
JoZu03	R. Joaquim, A. Zúuquet, S. Ferreira: „Revs - a robust electronic voting system“. In: IADIS International Journal WWW/Internet, vol. 1, no. 2. 2003. S. 47-63
JuCa02	A. Juels, D. Catalano, M. Jakobsson:„Coercion-resistant electronic elections“. In: Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05. ACM, 2005. S. 61-70
JuLe02	W. Juang, C. Lei, H. Liaw: „A verifiable multi-authority secret election allowing abstention from voting“. In: The Computer Journal, Vol. 45, No. 6, 2002. S. 672-682
JuLe97	W. Juang, C. Lei: „A Secure and Practical Electronic Voting Scheme for Real World Environments“. In: IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences Vol.E80-A No.1 1997. S. 64-71
KaKa05	H. Kaminski, L. Kari, M. Perry: „Who counts your votes?“. In: Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service, 2005. EEE '05. IEEE, 2005. S. 598-603
KaRu03	P. Karger, O. Rüß: „Sicherheit ist conditio sine qua non“. In: Institut für Informationsverarbeitung und Informationswissenschaft, Wirtschaftsuniversität Wien (Hrsg.): e-Voting in der Schweiz, Deutschland und Österreich: Ein Überblick, Nr. 02/2003, Wien. 2003. S. 17-21
KaWa99	J. Karro, J. Wang: „Towards a practical, secure, and very large scale online election“. In: Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC'99), IEEE Computer Society Press, 1999. S. 161-169
Keat04	D. Keating: „Pentagon's Online Voting Program Deemed Too Risky“. Washington Post. 22.1.2004, S. A01
Keig04	D. Keiger: „E-lective Alarm“. In: Johns Hopkins Magazine, February 2004. S. 50-56
Kerc83	A. Kerckhoffs: „La cryptographie militaire“, In: Journal des sciences militaires, vol. IX, S.

Kürzel	*Quelle*
	5-38, Jan. 1883, S. 161-191, Feb. 1883
KiKo06	A. Kiayias, M. Korman, D. Walluck: „An Internet Voting System Supporting User Privacy". In: Proceedings of the 22nd Annual Computer Security Applications Conference ACSAC '06. IEEE Computer Society, 2006. S. 165-174
KiSa03	N. Gong, A. Samsudin: „Incoercible Secure Electronic Voting Scheme Based on Chaffing and Winnowing". In: Conference on Communications, 2003. APCC 2003. The 9th Asia-Pacific, Vol.2, 2003. S. 838-843
Kitc04	J. Kitcat: „Source availability and e-voting: an advocate recants". In: Communications of the ACM. Volume 47, Issue 10 (October 2004). Voting systems. SPECIAL ISSUE: The problems and potentials of voting systems. 2004. S. 65-67
KiYu02	A. Kiayias, M. Yung: „Self-tallying Elections and Perfect Ballot Secrecy". In: Public Key Cryptography, Lecture Notes in Computer Science, Vol. 2274. Springer, 2002. S. 141-158
KiYu04	A. Kiayias, M. Yung: „The Vector-Ballot e-Voting Approach". In: Financial Cryptography, Lecture Notes in Computer Science, Vol. 3110. Springer, 2004. S. 72-89
KlKu05	M. Klonowski, M. Kutyłowski, A. Lauks, F. Zagórski: „A Practical Voting Scheme with Receipts". In: Lecture Notes in Computer Science, Vol. 3650. Springer, 2005. S. 490-497
Kneu06	R. Kneuper: „CMMI - Verbesserung von Softwareprozessen mit Capability Maturity Model Integration". 2. überarb. und erw. Aufl. dpunkt, 2006
KoSc04	P. Kocher, B. Schneier: „Insider risks in elections". In: Communications of the ACM, Volume 47, Issue 7. Column: Inside risks S. 104
KoSt04	T. Kohno, A. Stubblefield, A. Rubin: „Analysis of an Electronic Voting System". In: Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on 9-12 May 2004. 2004. S. 27-40
Krim02	R. Krimmer: „e-Voting.at - Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen". Working Papers on Information Processing and Information Management, Nr. 05/2002.
Krim03	R. Krimmer: „e-Voting in Österreich". In: „e-Voting in der Schweiz, Deutschland und Österreich: Ein Überblick". Working Papers on Information Processing and Information Management, Nr. 02/2003, Februar 2003. Internationales Rechtsinformatik Symposium - Session "e-Democracy/e-Voting". 2003. S. 29-33
KrVo05	R. Krimmer, M. Volkamer: „Wählen auf Distanz: Ein Vergleich zwischen elektronischen und nicht elektronischen Verfahren". In: E. Schweighofer; S. Augeneder; D. Liebwald; T. Menzel (Hrsg.). Effizienz von e-Lösungen in Staat und Gesellschaft, Tagungsband IRIS 2005, Salzburg, Österreich, Boorberg Verlag. 2005. S. 256-262
KuHo04	W. Ku, C. Ho: „An e-Voting Scheme against Bribe and Coercion". In: Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04), 2004. S. 113-116
KuRi07	C. Kurz, F. Rieger, R. Gonggrijp: „Beschreibung und Auswertung der Untersuchungen an NEDAP-Wahlcomputern". Berlin, 30. Mai 2007

Kürzel	*Quelle*
LaGr02	C. Lambrinoudakis, D. Gritzalis, S. Katsikas: „Building a reliable e-voting system: functional requirements and legal constraints“. In: Proceedings. 13th International Workshop on Database and Expert Systems Applications, 2002. S. 435-447
LaMo04	P. La Monica: „The trouble with e-voting - Political concerns have held back shares of Diebold, which makes touch screen voting machines.“ CNN Money.com, 30.08.2004
Land07	L. Landes: „The Landes Report: To Congress“. The Landes Report, Open Vote Project. 15.1.2007
Lann04	C. Lanner: „Verfassungsrecht - mit der Wahlrechtsnovelle 2003 (Herabsetzung des Wahlalters) und dem Kundmachungsreformgesetz 2004 - mit dem Bundesgesetzblattgesetz 2004 (Kundmachung des Bundesgesetzblattes im Internet) sowie dem Presseförderungsgesetz 2004, Änderungen insbesondere zu folgenden Rechtsvorschriften: Bundes-Verfassungsgesetz, Rundfunkgebührengesetz ...“. 20. Aufl., Stand: 1.2.2004. Wien: LexisNexis-Verl. ARD Orac. 2004
Lapr92	J. Laprie (ed.): „Dependability - basic concepts and terminology in English, French, German, Italian and Japanese“. Springer, 1992
LeBo04	B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, S. Yoo: „Providing Receipt-freeness in Mixnet-based Voting Protocols“. In: Information Security and Cryptology -ICISC 2003, Lecture Notes in Computer Science, Vol. 2971. Springer, 2004. S. 245-258
LeHa83	N. Leveson, S. Harvey: „Analyzing Software Safety“. In: Software Engineering, IEEE Transactions on, Volume SE-9, Issue 5. 1983. S. 569-579
LeKi00	B. Lee, K. Kim: „Receipt-free Electronic Voting through Collaboration of Voter and Honest Verifier“. In: Proceeding of JW-ISC2000, 2000. S. 101-108
LeKi03	B. Lee, K. Kim: „Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer“. In: Information Security and Cryptology — ICISC 2002, Lecture Notes in Computer Science, Vol. 2587. Springer, 2003. S. 389-406
Leve86	N. Leveson: „Software safety: why, what, and how“. In: ACM Computing Surveys (CSUR). Volume 18, Issue 2. 1986. S. 125-163
Leve95	N. Leveson: „Safeware: System Safety and Computers“. Reading, Addison-Wesley, 1995
Lope05	J. Penha-Lopes: „Why use an Open-Source e-voting system?“. In: Annual Joint Conference Integrating Technology into Computer Science Education. Proceedings of the 10th annual SIGCSE conference on Innovation and technology in computer science education. 2005. S. 412
Lund08	D. Lundin: „Component Based Electronic Voting Systems“. In: Dagstuhl Seminar Proceedings, Frontiers of Electronic Voting, Vol. 07311. IBFI, 2008
MaMa06	Ü. Madise, T. Martens: „E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world“. In: Proceedings of the 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC. Electronic Voting 2006. GI, 2006. S. 15-26
MaMa07	D. Malkhi, O. Margo, E. Pavlov: „E-voting without ‘Cryptography’“. In: Financial Cryptography,

Kürzel	*Quelle*
	Lecture Notes in Computer Science, Vol. 2357. Springer, 2007. S. 1-15
MaPo04	A. Maidou, H. Polatoglou: „E-Voting and the architecture of virtual space“. In: Proceedings of the 1st International Workshop on Electronic Voting. „Electronic Voting in Europe: Technology, Law, Politics and Society“. GI, 2004. S. 133-142
Mars00	W. Marschitz: „Die Zukunft des Wählens - Internet-voting“. In: Österreichische Monatshefte (Hg. ÖVP). Ausgabe 6/2000. S. 32ff
MaSt05	C. Mano, A. Streigel: „Introducing Security Analysis in Computer Security Courses Through an Electronic Voting Project“, In: Frontiers in Education, 2005. FIE '05. Proceedings 35th Annual Conference. 19-22 Oct. 2005. S. T2E- 12-16
McGr06	G. McGraw: „Software Security: Building Security in“. Addison-Wesley Professional. 2006
McLa05	L. McLaughlin: „Interview: Holistic Security“. In: Security & Privacy Magazine, IEEE. Volume 3, Issue 3. 2005. S. 6-8
MeHa07	M. Meyers, S. Harris: „CISSP - certified information systems security professional - das Zertifikat für IT-Sicherheit - die optimale Prüfungsvorbereitung“. Mitp, 2. Aufl., 2007
MeNe03	R. Mercuri, S. Neumann: „Security by obscurity“. In: Communications of the ACM, Volume 46, Issue 11 (November 2003). Blueprint for the future of high-performance networking. Column: Inside risks. 2003. S. 160
MeNe03a	R. Mercuri, S. Neumann: „Verification for electronic balloting systems“. In: Secure Electronic Voting. Kluwer Academic Publ., 2003. S. 31-42
Menz02	T. Menzel: „Rechtsgrundlage zur elektronischen Wahl“. In: Schweighofer, E.; Menzel, T.; Kreuzbauer, G. (Hrsg.): IT in Recht und Staat. Verlag Österreich. 2002, S. 123-133
Merc02	R. Mercuri: „A better ballot box?“. In: Spectrum, IEEE, Volume 39, Issue 10. 2002. S. 46-50
Merc05	R. Mercuri „Trusting in transparency“. In: Communications of the ACM Volume 48, Issue 5. 2005. S. 15-19
MiGr02	L. Mitrou, D. Gritzalis, S. Katsikas: „Revisiting legal and regulatory requirements for secure e-voting“. In: IFIP Conference Proceedings; Vol. 214, Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives. Kluwer Academics Publishers, 2002. S. 469-480
MoGl01	J. Mohen, J. Glidden: „The case for Internet Voting“. In: Communications of the ACM, January 2001/Vol. 44, No. 1. ACM, 2001. S. 72-85
move05	move moderne verwaltung: „T-Systems - Elektronische Betriebsratswahl“. 26.10.2005
MuVa98	Y. Mu, V. Varadharajan: „Anonymous secure e-voting over a network“. In: Computer Security Applications Conference, 1998, Proceedings., 14th Annual . S. 293-299
Nagy05	T. Nagy: „Sichere IT in der Wirtschaft“. In: A. Zechner (Hrsg.): E-Austria-Guide - E-Government, E-Learning, E-Health, E-Business. Linde, 2005. S. 186f
Neff04	C. Neff: „Practical High Certainty Intent Verification for Encrypted Votes“. DRAFT, October 14, 2004
NeMe00	P. Neumann, R. Mercuri, L. Weinstein: „Internet and Electronic Voting“. In: The Risks Digest,

Kürzel	*Quelle*
	Forum on Risks to the Public in Computers and Related Systems. ACM Committee on Computers and Public Policy, Volume 21, Issue 14. Tuesday 12 December 2000
OASI07	OASIS Organization for the Advancement of Structured Information Standards: „Report on the Election Markup Language (EML) Interoperability Demonstration held 29/30 October 2007 in Ditton Manor UK". 2007
OECD02	OECD Organisation For Economic Co-Operation And Development: „Guidelines for the Security of Information Systems and Networks - Towards A Culture Of Security". 2002
OgKu97	W. Ogata, K. Kurosawa, K. Sako, K. Takatani: „Fault Tolerant Anonymous Channel". In: Information and Communications Security ICICS '97, Lecture Notes in Computer Science, Vol. 1334. Springer, 1997. S. 440-444
OhMi99	M. Ohkubo, F. Miura, M. Abe, A. Fujioka, T. Okamoto: „An Improvement on a Practical Secret Voting Scheme Source". In: Proceedings of the 2nd International Workshop on Information Security, Lecture Notes in Computer Science, Vol. 1729. Springer, 1999. S. 225-234
Okam96	T. Okamoto: „An Electronic Voting Scheme". In: Proceedings of IFIP'96, Advanced IT Tools, Chapman and Hall, 1996. S. 21-30
Okam97	T. Okamoto: „Receipt-free electronic voting schemes for large scale elections". In: Proceedings of Workshop on Security Protocols '97, Lecture Notes in Computer Science, Vol. 1361. Springer, 1997. S. 25-35
OlGa06	A. Oliva, S. García, E. Belleboni: „Contributions to traditional electronic voting systems in order to reinforce citizen confidence". In: Proceedings of the 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC. Electronic Voting 2006. GI, 2006. S. 39-49
OnGr05	B. Ondrisek, T. Grechenig, S. Leitner: „Eine prototypische Diskussion von M-Voting am Fallbeispiel der Wahl zum österreichischen Bundespräsidenten". In: IRIS 2005. Effizienz von e-Loesungen in Staat und Gesellschaft. Aktuelle Fragen der Rechtsinformatik. Richard Borberg Verlag, 2005. S. 290-297
OoBe04	A. Oostveen, S. Besselaar: „Security as belief - User's perceptions on the security of electronic voting systems". In: Proceedings of the 1st International Workshop on Electronic Voting. „Electronic Voting in Europe: Technology, Law, Politics and Society". GI, 2004. S. 73-82
ORG07	ORG Open Rights Group: „May 2007 Election Report - Findings of the Open Rights Group Election Observation Mission in Scotland and England". 20 Juni 2007
OSCE07	OSCE Office for Democratic Institutions and Human Rights: „Belgium - Federal Elections 10 June 2007". OSCE/ODIHR Needs Assessment Mission Report. Warsaw, 19 October 2007
Over06	S. Overton: „Stealing Democracy: The New Politics of Voter Suppression". W. W. Norton. 2006
Pail99	P. Paillier: „Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: Advances in Cryptology - EUROCRYPT'99, Lecture Notes in Computer Science, Vol. 1592. Springer, 1999. S. 223-238

Kürzel	*Quelle*
PaIt93	C. Park, K. Itoh, K. Kurosawa. „Efficient anonymous channel and all/nothing election scheme“. In: Advances in Cryptology - EUROCRYPT '93, Lecture Notes in Computer Science., Vol. 765. Springer, 1993. S. 248-259
Parh94	B. Parhami: „Voting Algorithms“. In: IEEE Transactions on Reliability, Vol. 43, NO. 4, 1994 December. IEEE, 1994. S. 617-629
PaSh06	H. Park, D. Shin: „Intelligent Anonymous Secure E-Voting Scheme“. In: Knowledge-Based Intelligent Information and Engineering Systems, Lecture Notes in Computer Science, Vol. 4252. Springer, 2006. S. 726-736
PeAd04	K. Peng, R. Aditya, C. Boyd, E. Dawson, B. Lee: „Multiplicative Homomorphic E-Voting“. In: Proceedings of INDOCRYPT 2004, Lecture Notes in Computer Science, Vol. 3348. Springer, 2004. S. 61-72
PfPf03	C. Pfleeger, S. Pfleeger: „Security in computing“. 3. ed. Prentice Hall PTR, 2003
Phil02	M. Philippsen: „Internetwahlen - Demokratische Wahlen über das Internet?“. In: Informatik Spektrum, Vol. 25, Issue 2. 2002. S. 138-150
Pipe97	F. Piper: „Encryption“. In: Proceedings of the European Conference on Security and Detection, Conference Publication No. 437. IEEE, 1997. S. 61-5
PoKo02	M. Pol, T, Koomen, A. Spillner: „Management und Optimierung des Testprozesses: ein praktischer Leitfaden für erfolgreiches Testen von Software, mit TPI und Tmap“. 2., aktualisierte Auflage. dpunkt. 2002
Poor99	R. Poore: „Generally Accepted System Security Principles - Release for Public Comment“. In: Information systems security, Vol. 8, N. 3. Auerbach, 1996. S. 27-77
PrKo02	A. Prosser, R. Kofler, R. Krimmer: „Deploying Electronic Democracy for Public Corporations“. In: Traunmüller, R. (ed.): Electronic Government, Lecture Notes in Computer Science 2739. Springer, 2003. S. 234-239
PrKo04	A. Prosser, R. Kofler, R. Krimmer, M. Unger: „e-Voting Wahltest zur Bundespräsidentschaftswahl 2004“, Arbeitsbericht zum Tätigkeitsfeld Wirtschaftsinformatik, Informationsverarbeitung und Informationswirtschaft 01/2004, Wirtschaftsuniversität Wien, 2004
PrMu02	A. Prosser, R. Müller-Török: „E-Democracy. Eine neue Qualität im demokratischen Entscheidungsprozess“. In: Wirtschaftinformatik Nr. 44. 2002. S. 545-56
PrSt06	A. Prosser, R. Steininger: „e-voting2006.at - An Electronic Voting Test Among Austrians Abroad“. Working Papers on Information Systems, Information Business and Operations, Nr. 02/2006
PTB04	PTB Physikalisch-Technische Bundesanstalt: „Prüfbericht der PTB vom 12.05.2004. Baumusterprüfung eines Wahlgerätes: ESD1 - Prüfbericht PTB-8.51-001.04“. 2004
Ques04	W. Quesenbery „Oops, They Forgot the Usability: Elections as a Case Study“. Michigan State University Conference on Usable Information Technology, 2004
RABA04	RABA Innovative Solution Cell: „Trusted Agent Report - Diebold AccuVote-TS Voting System“. January 20, 2004

Kürzel	*Quelle*
RaRa01	I. Ray, I. Ray, N. Narasimhamurthi: „An Anonymous Electronic Voting Protocol for Voting Over The Internet“. In: Proceedings of the 3rd International Workshop on Advanced Issues of E-Commerce and Web-based Information Systems (WECWIS '01), 2001. S. 180-190
Raym01	E. Raymond: „The Cathedral and the Bazaar Musings - on Linux and Open-Source by an Accidental Revolutionary“. 2001
Reas94	J. Reason: „Menschliches Versagen“. Spektrum Akademischer Verlag. 1994
Rech99	E. Rechtin: „Systems Architecting of Organizations. Why Eagles can't Swim“. In: CRC Press Inc. 1999
Redm98	F. Redmill: „IEC 61508-principles and use in the management of safety“. In: Computing & Control Engineering Journal. Volume 9, Issue 5, Oct. 1998. S. 205-213
Reis05	C. Reissner: „Elektronische Signatur und Bankkarte“. In: A. Zechner (Hrsg.): E-Austria-Guide - E-Government, E-Learning, E-Health, E-Business. Linde, 2005. S. 186f
Reze04	P. Rezende: „Electronic Voting Systems - Is Brazil ahead of its time?“. In: Cryptobytes, Vol 7, N. 2, RSA Security Laboritories, USA. 2004
RiSc08	F. Ricca, A. Scozzari, B. Simeone: „Weighted Voronoi Region Algorithms For Political Districting“. In: Dagstuhl Seminar Proceedings, Frontiers of Electronic Voting, Vol. 07311. IBFI, 2008
RiSh78	R. Rivest, A. Shamir, L. Adleman: „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems“. In: Communications of the ACM, Vol. 21 (2), 1978. S. 120-126
Rive06	R. Rivest: „The ThreeBallot Voting System“. Unpublished draft, Oct. 2006
RiWa06	R. Rivest, J. Wack: „On the notion of “software independence” in voting systems“. DRAFT Version 28.7.2006
Robe05	S. Robertson: „Voter-centered design: Toward a voter decision support system“. In: ACM Transactions on Computer-Human Interaction (TOCHI). Volume 12, Issue 2. 2005. S. 263-292
Rodr06	J. Filho: „E-Voting in Brazil - The Risks to Democracy“. In: Proceedings of the 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC. Electronic Voting 2006. GI, 2006. S. 85-94
Rose00	S. Rosenberger: „Wahlen und Parteien“. Medienpaket Politische Bildung. Wien: AWS/Manz. Kapitel 4. 2000
Rosl04	G. Røsland: „Remote Electronic Voting“ . 20.05.2004. Report Universität Bergen
RoWe89	A. Roßnagel, S. Wedde, V. Hammer, U. Pordesch: „Die Verletzlichkeit der 'Informationsgesellschaft'“. VS Verlag für Sozialwissenschaften, 1989
Rubi02	A. Rubin: „Security considerations for remote electronic voting“. Communications of the ACM, Volume 45, Issue 12. ACM, 2002. S. 39-44
Rubi06	A. Rubin: „Brave new ballot - the battle of safeguard democracy in the age of electronic voting“. Morgan Road Books. 2006
RySc06	P. Ryan, S. Schneider. „Prêt à Voter with Re-encryption Mixes“. In: Computer Security - ESORICS, Lecture Notes in Computer Science, Vol. 4189. Springer, 2006 S. 313-326
SAIC03	SAIC Science Applications International Corporation: „Risk Assessment Report - Diebold Ac-

Kürzel	*Quelle*
	cuVote-TS Voting System and Processes“. State of Maryland. September 2, 2003
Sail07	M. Sailhan: „Voting machines a 'catastrophe'--French parties“. Inquirer.net 23.04.2007
SaKi94	K. Sako, J. Kilian. „Secure Voting Using Partially Compatible Homomorphisms“. In: Advances in Cryptology — CRYPTO ’94. Lecture Notes in Computer Science Volume, 839. Springer, 1994. S. 411-424
SaKi95	K. Sako, J. Kilian. „Receipt-free mix-type voting scheme - A practical solution to the implementation of a voting booth“. In: Advances in Cryptology - EUROCRYPT '95, Lecture Notes in Computer Science, Vol. 921. Springer, 1995. S. 393-403
SaKo06	N. Sastry, T. Kohno, D. Wagner: „Designing Voting Machines for Verification“. In: Proceedings of the 15th USENIX Security Symposium. 2006. S. 321-336
Salt06	R. Saltman: „The History and Politics of Voting Technology - in quest of integrity and public confidence“. 1. ed. Palgrave Macmillan, 2006
Salt88	R. Saltman: „Accuracy, integrity and security in computerized vote-tallying“. In: Communications of the ACM. Volume 31, Issue 10. 1988. S. 1184-1191
SaPo06	K. Sampigethaya, R. Poovendran: „A framework and taxonomy for comparison of electronic voting schemes“. In: Computers & Security. Vol. 25. No. 2. Elsevier 2006. S. 137-153
Sche01	K. Schedler: „eGovernment und neue Servicequalität der Verwaltung?“. In: eGovernment. Eine Standortbestimmung. Bern. 2001. S. 33-51
Schl00	M. Schlifni: „Electronic voting systems and electronic democracy - participatory e-politics for a new wave of democracy“. Dissertation TU Wien. 2000
Schn00	B. Schneier: „Inside risks: semantic network attacks“. In: Communications of the ACM, Volume 43, Issue 12 (December 2000). 2000. S. 168
Schn04	B. Schneier: „Secrets & lies - IT-Sicherheit in einer vernetzten Welt“. dpunkt-Verl., 2004
Schn96	B. Schneier: „Applied cryptography - protocols, algorithms, and source code in C“. 2. ed. 1996
Schn99	B. Schneier: „Attack Trees - Modeling security threats“. In: Dr. Dobb's Journal of Software Tools 24, 12. 1999. S. 21-9
Scho99	B. Schoenmakers: „A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting“. In: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, Lecture Notes in Computer Science. Vol. 1666. Springer, 1999. S. 148-164
Schu03	M. Schumacher: „Introduction“. In: Security Engineering with Patterns - Origins, Theoretical Models, and New Applications. Lecture Notes in Computer Science, Vol. 2754. Springer, 2003. S. 1-9
Schu03a	M. Schumacher: „The Human Factor“. In: Security Engineering with Patterns - Origins, Theoretical Models, and New Applications. Lecture Notes in Computer Science, Vol. 2754. Springer, 2003. S. 45-55
Schw04	J. Schwartz: „Glitch Found in Ohio Counting“. New York Times, 6. November 2004
Sham04	M. Shamos: „Paper v. Electronic Voting Records - An Assessment“. In: Proceedings of the

Kürzel	*Quelle*
	14th ACM Conference on Computers, Freedom and Privacy. 2004
Sham79	A. Shamir: „How to share a secret“. In: Communications of the ACM, Volume 22, Issue 11. ACM, 1979. S. 612-613
Sham93	M. Shamos: „Electronic Voting - Evaluating the Threat“. In: Proceedings of the 3rd ACM Conference on Computers, Freedom, and Privacy. ACM, 1993
Siet05	R. Sietmann: „Dreimal drücken - fertig? - E-Voting-Großeinsatz bei der Bundestagswahl“. c't 19/2005. S. 54
Siet06	R. Sietmann: „Schach dem E-Voting - Hackerteam demonstriert die Manipulierbarkeit von Wahlcomputern“. c't 22/2006, S. 52
Siet07	R. Sietmann: „Wähler-Selbstkontrolle - Experten ringen um Vertrauen in elektronische Wahlmaschinen“. c't 19/2007. S. 84
Simo04	B. Simons: „Electronic voting systems: the good, the bad, and the stupid“. In: Queue Volume 2, Issue 7 (October 2004). RFID: threat or promise? Department: Opinion. 2004. S. 20-26
Somm01	I. Sommerville: „Software Engineering“. 6. Auflage. Pearson Studium. 2001
Somm06	I. Sommerville: „Software Engineering“. (Engl.) 8. Auflage. Pearson Studium. 2006
Somm07	I. Sommerville: „Software Engineering“. (Deutsche) 8. Auflage. Pearson Studium. 2007
Song06	M. Songini: „Paper Trail Flawed in Ohio Election, Study Finds“. Computerworld August 21, 2006
Spar01	D. Spar „Ruling the Waves: Cycles of Discovery, Chaos, and Wealth, from the Compass to the Internet“. Harcourt, 2001
Stab02	Stabsstelle IKT-Strategie des Bundes: „Das Österreichische IT-Sicherheitshandbuch“. Version 2.2, Bundeskanzleramt. 2002
StDu05	T. Storer, I. Duncan: „Two Variations to the mCESG Pollsterless e-Voting Scheme“. In: Proceedings of the 29th Annual International Computer Software and Applications Conference (COMPSAC'05). IEEE, 2005. S. 425-430 Vol. 2
StDu98	V. Stavridou, B. Dutertre: „From security to safety and back“. In: Proceedings of Computer Security, Dependability and Assurance: From Needs to Solutions. IEEE, 1998. S. 182-195
Ston03	A. Stone: „E-Voting: Should We Pull the Lever?“. In: Software, IEEE. Nov.-Dec. 2003 Volume: 20, Issue: 6. 2003. S. 12-14
StWe05	R. Stein, G. Wenda: „E-Voting in Österreich: Status Quo und Ausblick“. Ausgabe 3/2005 des .SIAK-Journals, der wissenschaftlichen Zeitschrift des BM.I. 2005
SwSn04	F. Swiderski, W. Snyder: „Threat Modeling“. Microsoft Press. Reihe „Microsoft Professional (silberne Reihe)“. 1. Auflage. 2004
Tane95	A. Tanenbaum: „Distributed Operating Systems“. Prentice Hall, 1995.
TaSt02	A. Tanenbaum, M. van Steen: „Distributed systems - principles and paradigms“. Prentice Hall, 2002
TjPe07	T. Tjøstheim, T. Peacock, S. Ryan: „A Case Study in System-Based Analysis: The ThreeBallot Voting System and Prêt à Voter“. In: Proceedings of VoComp 2007
TSys08	T-Systems Media Relations: „Online-Wahlen - Das Internet als Wahllokal“. Presseaussendung

Kürzel	*Quelle*
	Bonn, 20. Letzter Stand: 25. Januar 2008
UlKo01	M. Ullmann, F. Koob, F. Schulz: „Online-Wahlen: Skizze einer Security Policy“. In: „2001 - Odyssee im Cyberspace? - Sicherheit im Internet“. Tagungsband 7. Deutscher IT-Sicherheits-kongress des BSI 2001 / Bundesamt für Sicherheit in der Informationstechnik. SecuMedia-Verl., 2001- S. 181-195
USAT04	USA Today: „More than 4,500 North Carolina votes lost because of mistake in voting machine capacity“. April 2004
Vene02	Europäische Kommission für Demokratie durch Recht (Venedig-Kommission): „Verhaltensko-dex für Wahlen - Leitlinien und Erläuternder Bericht“. 51. und 52. Tagung der Venedig-Kom-mission. Bundesministerium der Justiz, Mitteilung Nr. 190/2002, CDL-AD (2002) Straßburg, den 30. Oktober. 2002
VfGH85	VfGH Verfassungsgerichtshof: Das Erkenntnis vom 16.03.1985. Sammlungsnummer 10412, Geschäftszahl G18/85, Dokumentnummer JFT/10149684/85G00018, Index L0 Verfassungs- und Organisationsrecht. 1985
VfGH89	VfGH Verfassungsgerichtshof: Das Erkenntnis vom 16.03.1989. Sammlungsnummer 12023, Geschäftszahl G218/88, Dokumentnummer JFR_10109684_88G00218_01. Index 10 Ver-fassungsrecht 10/04 Wahlen. 1989
VoGr06	M. Volkamer, R. Grimm: „Multipe Cast in Online-Voting“. In: Proceedings of the 2nd Interna-tional Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC. Electronic Voting 2006. GI, 2006. S. 97-106
VoKr06	M. Volkamer, R. Krimmer: „Die Online-Wahl auf dem Weg zum Durchbruch“. In: Informatik Spektrum 29 (2), 2006. S. 98-113
WaCo02	A. Watson, V. Cordonnier: „Voting in the New Millennium: eVoting Holds the Promise to Ex-pand Citizen Choice“. In: Proceedings of the First International Conference on Electronic Go-vernment, Lecture Notes in Computer Science, Vol. 2456. Springer, 2002. S. 234-239
WaLe04	C. Wang, H. Leung: „A Secure and Fully Private Borda Voting Protocol with Universal Verifia-bility“. In: Proceedings of the 28th Annual International Computer Software and Applications Conference (COMPSAC'04) - Volume 01, 2004. S. 224-229
WaLe05	C. Wang, H. Leung: „A Secure Voter-Resolved Approval Voting Protocol over Internet“. In: ACM International Conference Proceeding Series; Vol. 113. Proceedings of the 7th internatio-nal conference on Electronic commerce. ACM, 2005. S. 646-652
WaMa00	R. Walter, H. Mayer: „Grundriß des österreichischen Bundesverfassungsrechts“. 9. Auflage, durchges. und erg. Aufl. Manz, 2000
Wein00	L. Weinstein: „Inside risks: Risks of Internet voting“. In: Communications of the ACM, Volu-me 43, Issue 6. ACM, 2000. S. 128
WeVi07	K. Weldemariam, A. Villafiorita, A. Mattioli: „Assessing Procedural Risks and Threats in e-Vo-ting: Challenges and an Approach“. In: E-Voting and Identity, Lecture Notes in Computer Science. Vol. 4896. Springer. 2007. S. 38-49

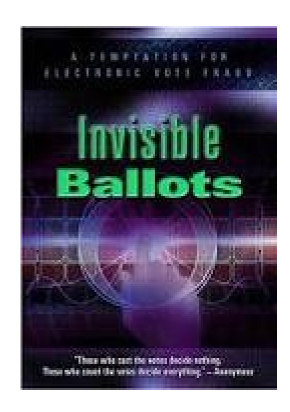
Kürzel	*Quelle*
WKG98	Wirtschaftskammergesetz 1998 - WKG. Bundesgesetz über die Kammern der gewerblichen Wirtschaft (Wirtschaftskammergesetz 1998 - WKG). BGBl. I Nr. 103/1998 i. d. F. BGBl. I Nr. 78/2006
Woeh04	J. Woehr: „A Conversation with Avi Rubin - DDJ contributing editor Jack Woehr talks to Avi Rubin, the world's leading authority on electronic voting and software engineering." Reprinted, with permission, from IEEE Symposium on Security and Privacy, 2004. 2004 IEEE. Dr. Dobb's Journal, Nov 01, 2004.
WOWT04	WOWT: „Countinghouse Blues - Too many votes". NBC WOWT T.V. Channel 6, Omaha, November 2004
XeMa04	A. Xenakis, A. Macintosh: „Levels of Difficulty in Introducing E-Voting". In: Proceedings of Third International Conference in E-Government, EGOV 2004; 30. August bis 3. September 2004, Zaragoza. 2004. S. 2
XeMa04a	A. Xenakis, A. Macintosh: „Trust in Public Administration e-Transactions: E-Voting in the UK". In: Proceedings of TrustBus 2004, DEXA 2004; Zaragoza, Spain; 30th August to 3rd September. 2004. S. 1ff
XeMa04b	A. Xenakis, A. Macintosh: „Procedural Security in Electronic Voting". In: System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on 5-8 Jan. IEEE, 2004. S. 8ff
XeMa04c	A. Xenakis, A. Macintosh: „Procedural security analysis of electronic voting". In: Rauterberg, M. (ed.) ICEC 2004. Lecture Notes in Computer Science, Vol. 3166. Springer, 2004. S. 541-546
XeMa05	A. Xenakis, A. Macintosh: „E-electoral Administration: Organizational Lessons Learned from the Deployment of E-voting in the UK". In: Vol. 89. Proceedings of the 2005 national conference on Digital government research. Atlanta, Georgia. SESSION: E-voting. 2005. S. 191-197
XeMa05a	A. Xenakis, A. Macintosh: „Procedural Security and Social Acceptance in E-voting". In: Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 5 - Volume 05. 2005. S. 118.1
YuLe03	S. Yun, S. Lee: „An Electronic Voting Scheme based on Undeniable Blind Signature Scheme". In: Proceedings of the IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003. S. 163-167
YuLe04	S. Yun, S. Lee: „The network based electronic voting scheme suitable for large scale election". In: Proceedings of the 6th International Conference on Advanced Communication Technology, 2004. S. 218-222
Zett04	K. Zetter: „E-Vote Glitch Inflates Bush Total". Wired Magazine, Politics : Security. 11.05.04
Zett04a	K. Zetter: „E-Vote Snafu in California County". Wired Magazine, Politics : Security. 03.19.04

Appendix D: Filmempfehlungen

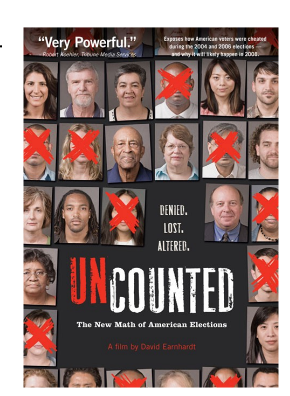
Film1 Hacking Democracy (2006)
Regie: Simon Ardizzone, Russell Michaels
Genre: Dokumentarfilm
Working Title: „Votergate“



Film2 Invisible Ballots (2004)
Regie: William Gazecki
Genre: Dokumentarfilm



Film3 Uncounted - The New Math of American Elections (2008)
Regie: David Earnhardt
Genre: Dokumentarfilm



Appendix E: Lebenslauf



Mag.rer.soc.oec. Dipl.-Ing. Barbara Ondrisek schrieb ihre Dissertation am Institut für Gestaltungs- und Wirkungsforschung, Arbeitsbereich Human Computer Interaction.

Ausbildung

Mittelschule: BG Gänserndorf (AHS) 1990-1998, Abschluss: Matura mit gutem Erfolg

Universität:

- Technische Universität Wien, Studienrichtung Informatik 1999-2004, Abschluss Dipl.-Ing. mit der Diplomarbeit „Entwurf und Realisierung eines Prototyps für Mobile Government am Beispiel von mobilen Wahlen"
- Technische Universität Wien, Studienrichtung Informatikmanagement 2006-2007, Abschluss Mag.rer.soc.oec.

Publikationen

- B. Ondrisek: „Sicherheit von E-Voting-Systemen". Angenommen für DACH Security 2008, Technische Universität Berlin, 24-25 Juni 2008
- B. Ondrisek, T. Grechenig, S. Leitner: „Eine prototypische Diskussion von M-Voting am Fall-beispiel der Wahl zum österreichischen Bundespräsidenten". In: IRIS 2005. Effizienz von e-Loesungen in Staat und Gesellschaft. Aktuelle Fragen der Rechtsinformatik. Richard Borberg Verlag, 2005. S. 290-297

Beruflicher Werdegang

- 03/07-heute: Bundesministerium für Landesverteidigung, Software- und Webentwicklung
- 04/05-09/06: Knallgrau New Media Solutions GmbH, Software- und Webentwicklung
- 04/04-03/05: Telekom Austria AG, Software- und Webentwicklung